Dedicated to innovation in aerospace

Towards dynamic cyber security risk assessment of military aircraft

Piet Hoogeboom
(Theo Verhoogt, René Wiegers, Judith van Bruggen, Nikita Noskov)

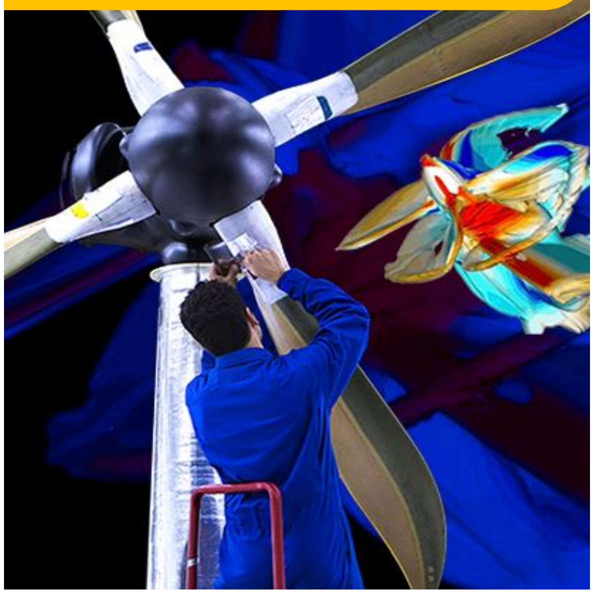
Overview

- NLR short overview
- Cyber security risk assessment methodology
  - Common elements
  - Layered approach
- Likelihood & example

Netherlands Aerospace Centre

- Non-profit foundation, supporting
  - Government & Industry
  - civil & military operations
- 600 employees
- €73 M revenue, 75% NLD, 21% EU, 4% international

- Aerospace vehicles



- Aerospace systems

- Aerospace operations

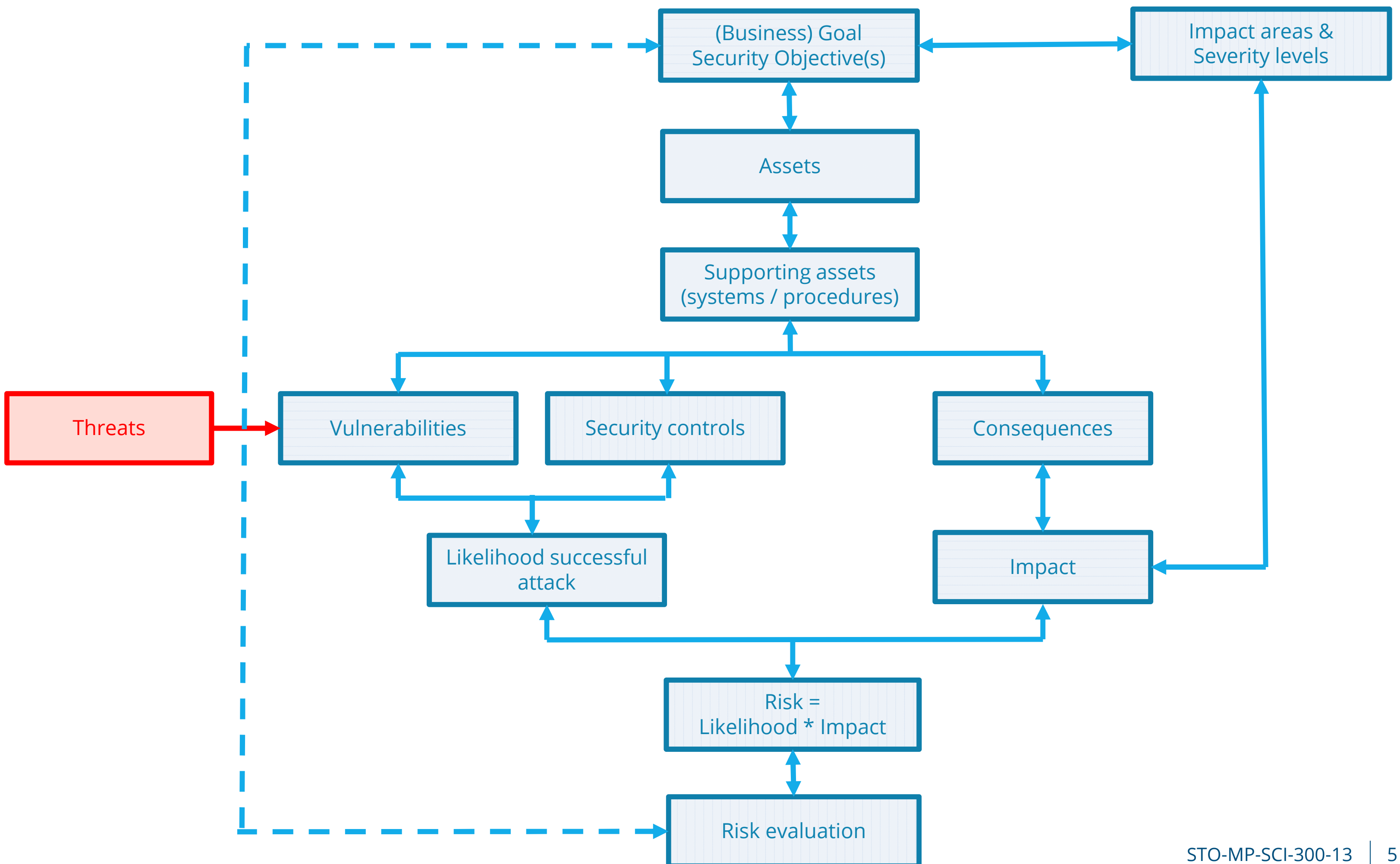
Security Risk Assessment (SRA)

- Many SRA methodologies exist
  - Optimised for specific domain and/or application

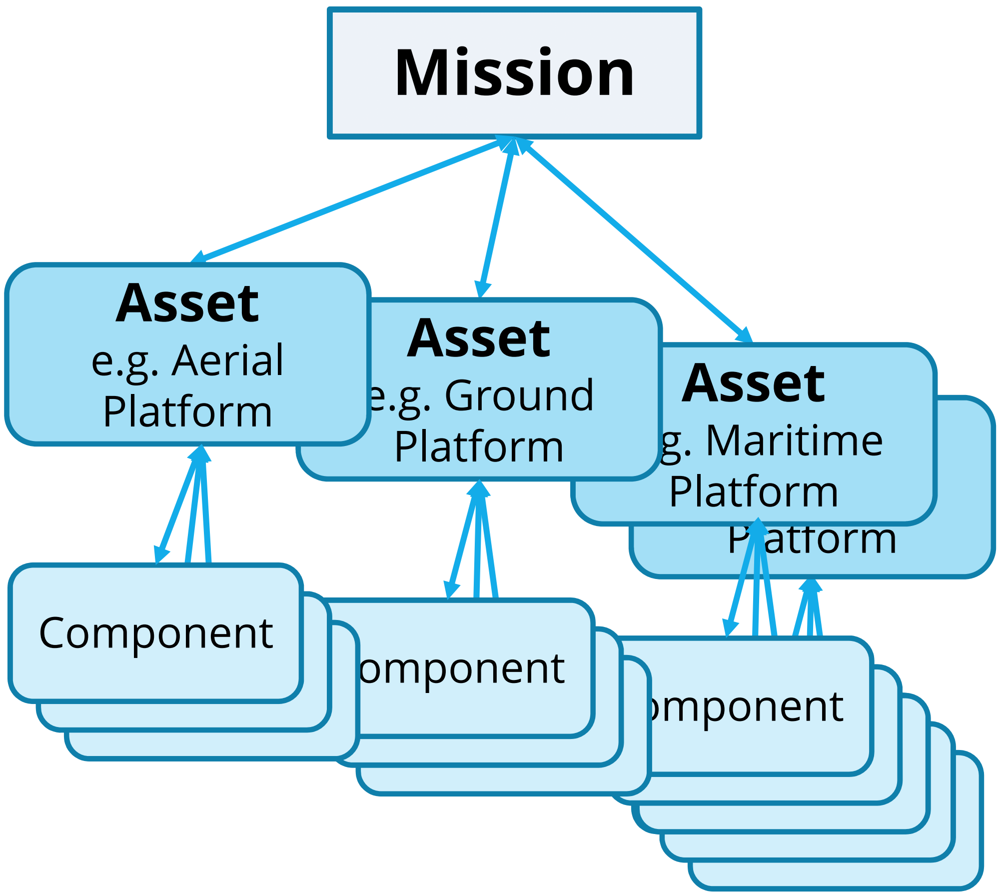
- A high level SRA framework as communication mechanism is needed

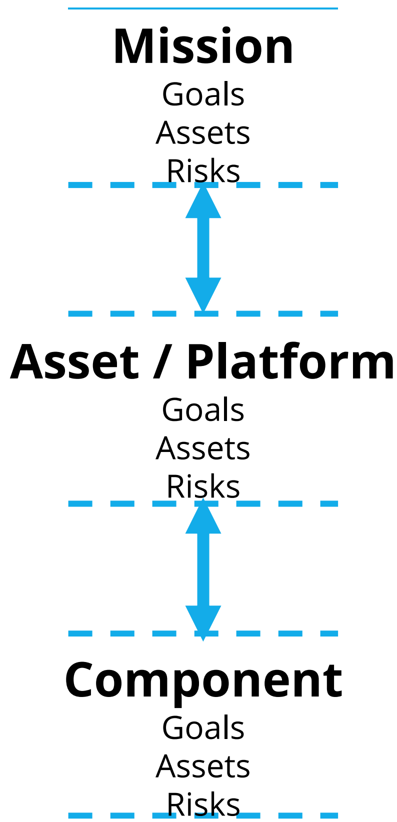
- Each domain/organisation has its own (unique) security requirements and knowledge about security issues
  - No open communication about existing vulnerabilities
  - Many known attacks including details (e.g. internet)
    - Sophistication increases continuously

SRA common elements

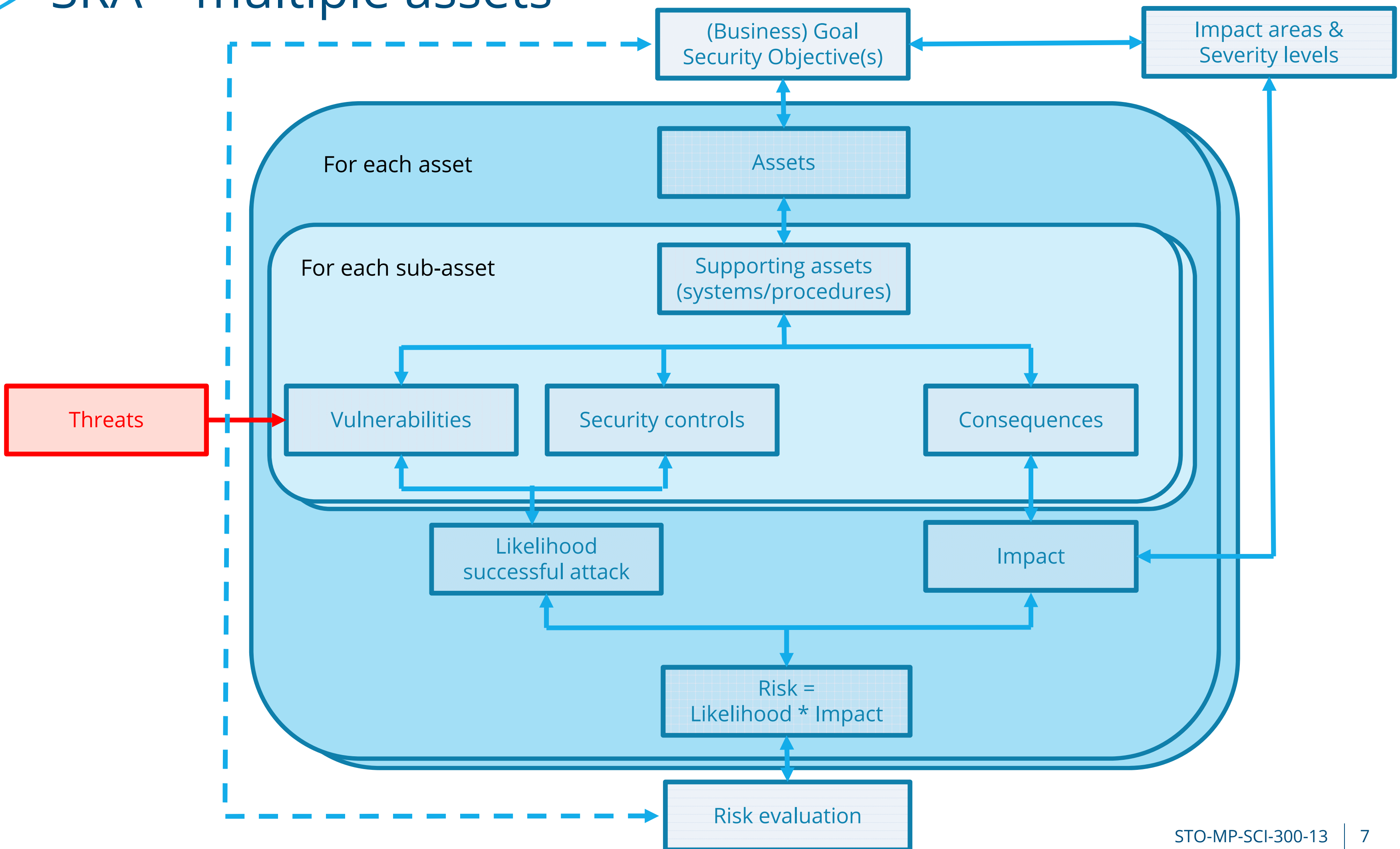


SRA – multiple assets & levels

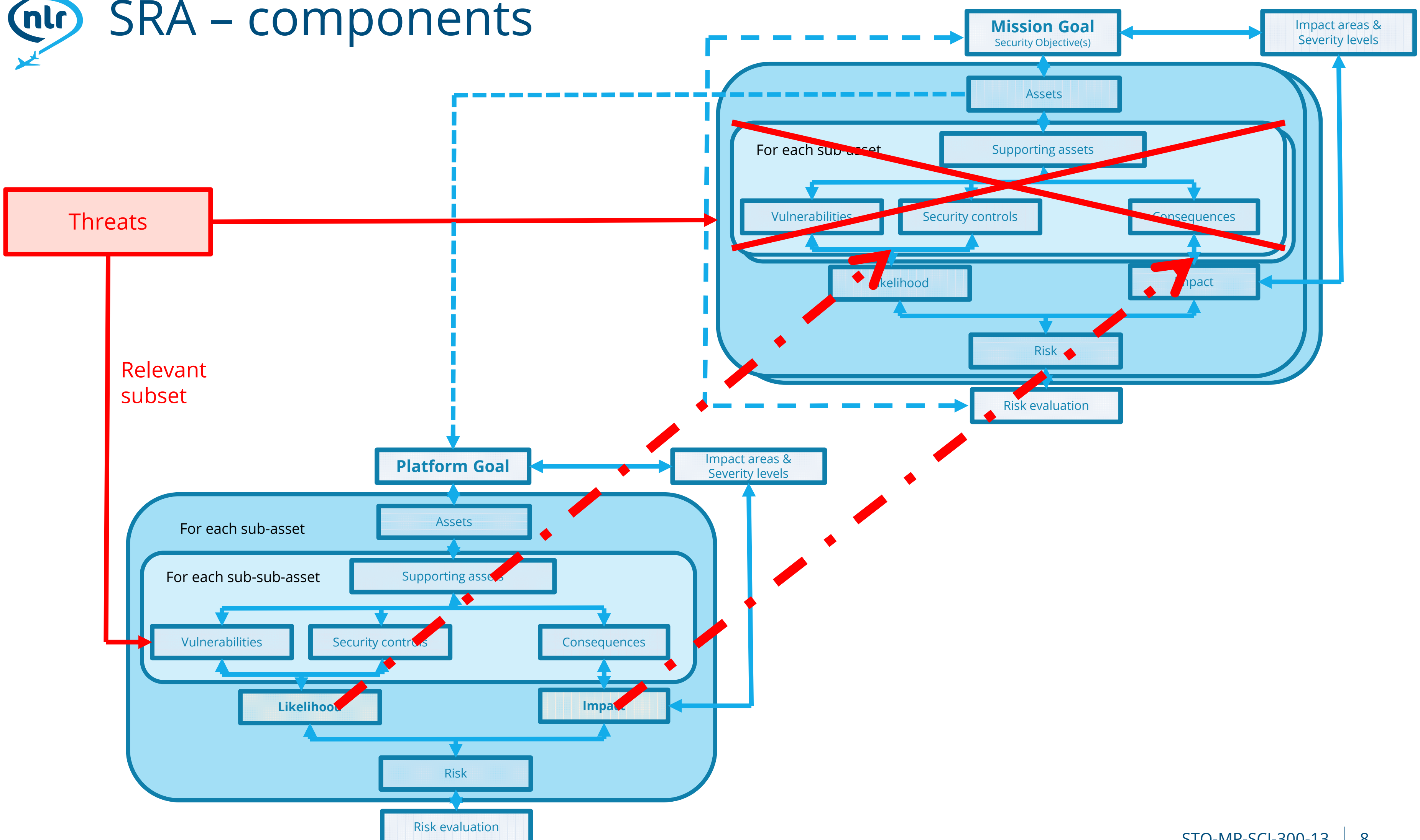




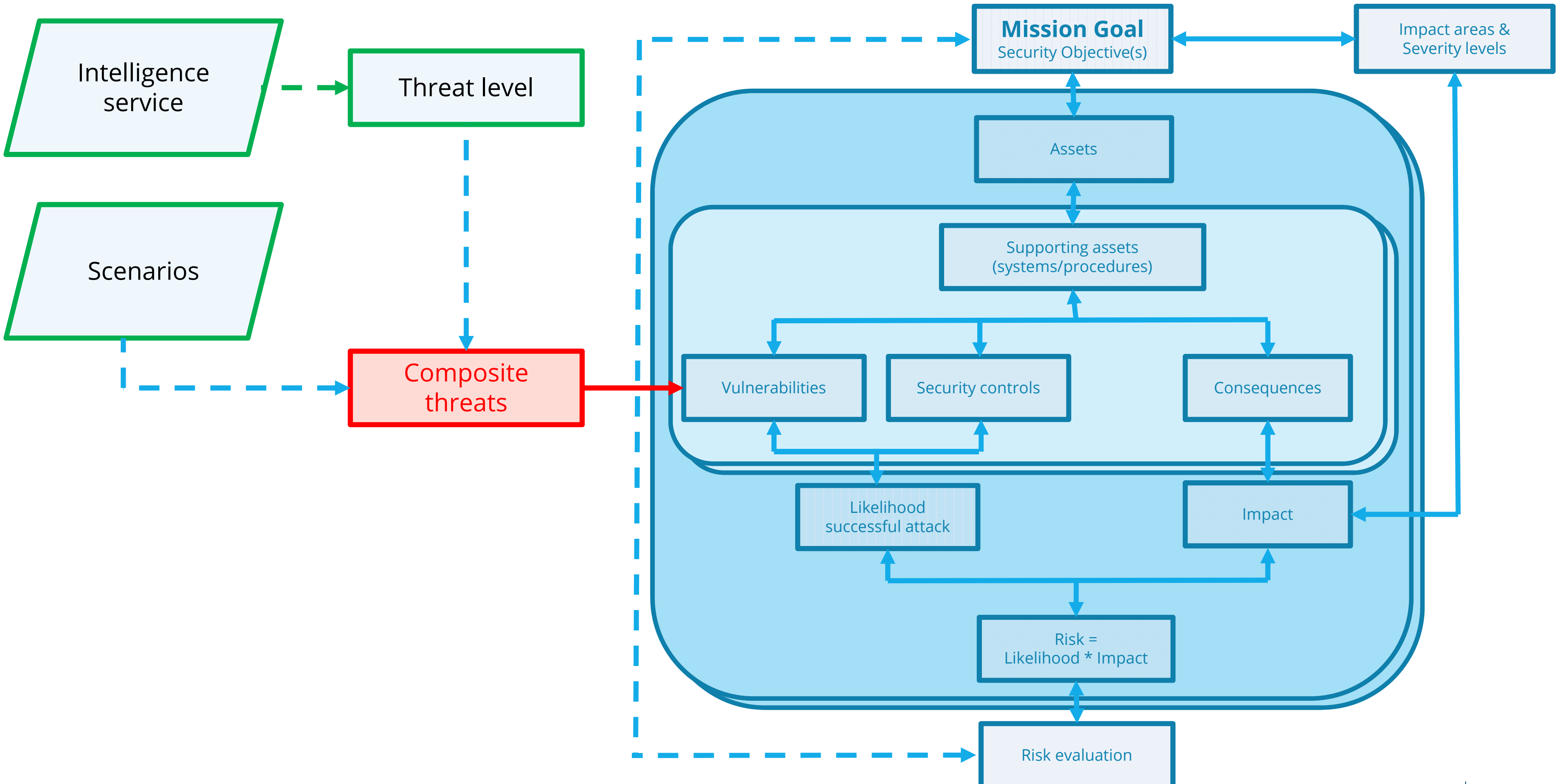
SRA – multiple assets



SRA – components

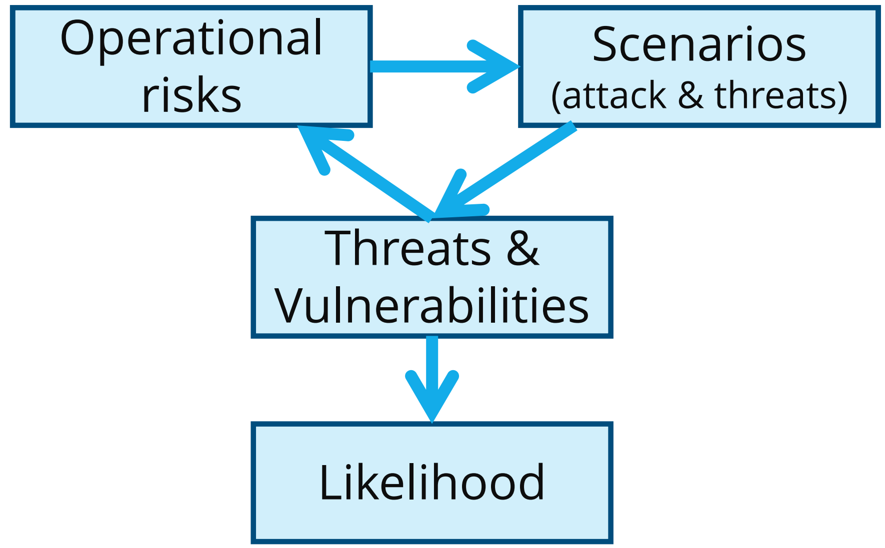


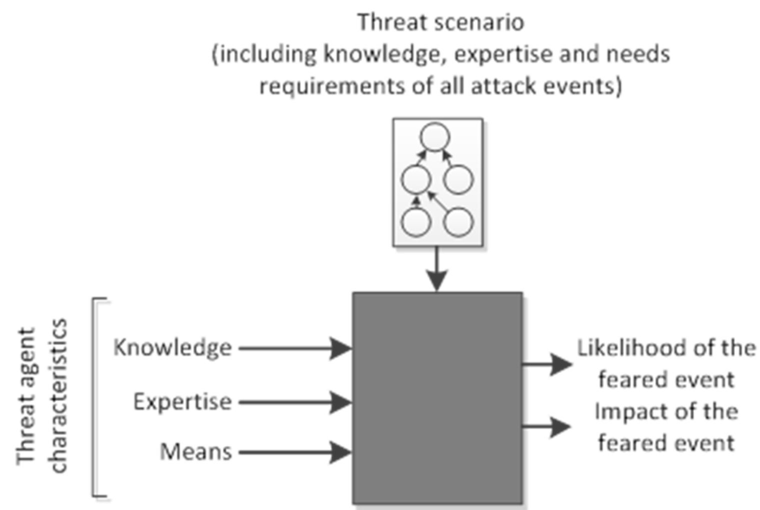
SRA – multiple threats



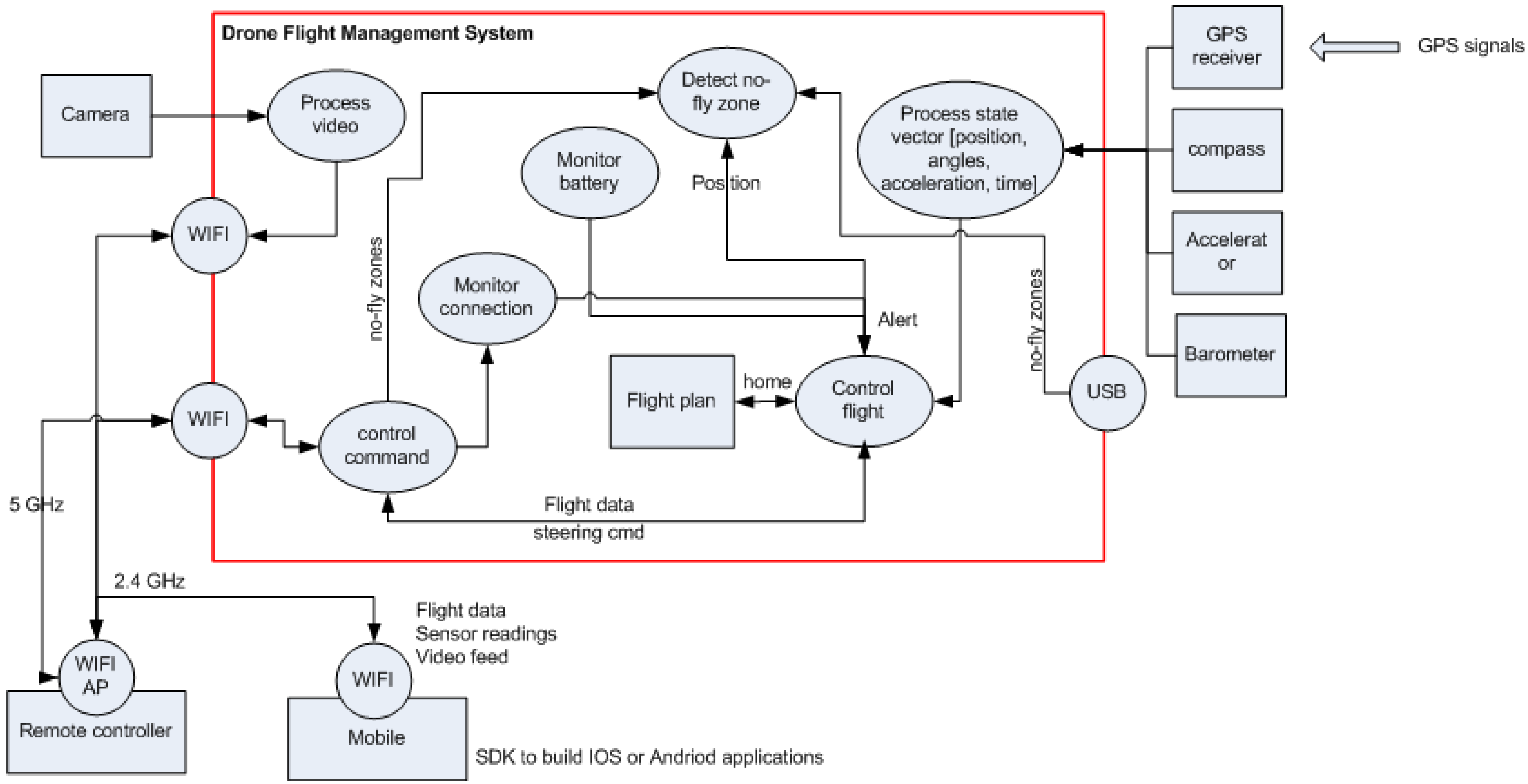
Security risk assessment

- Feared events / Operational risks
  - E.g. divert from intended mission
- Composite threats
  - Which combinations of threats lead to a potential feared event (scenario)
- Likelihood estimation
- Impact rating

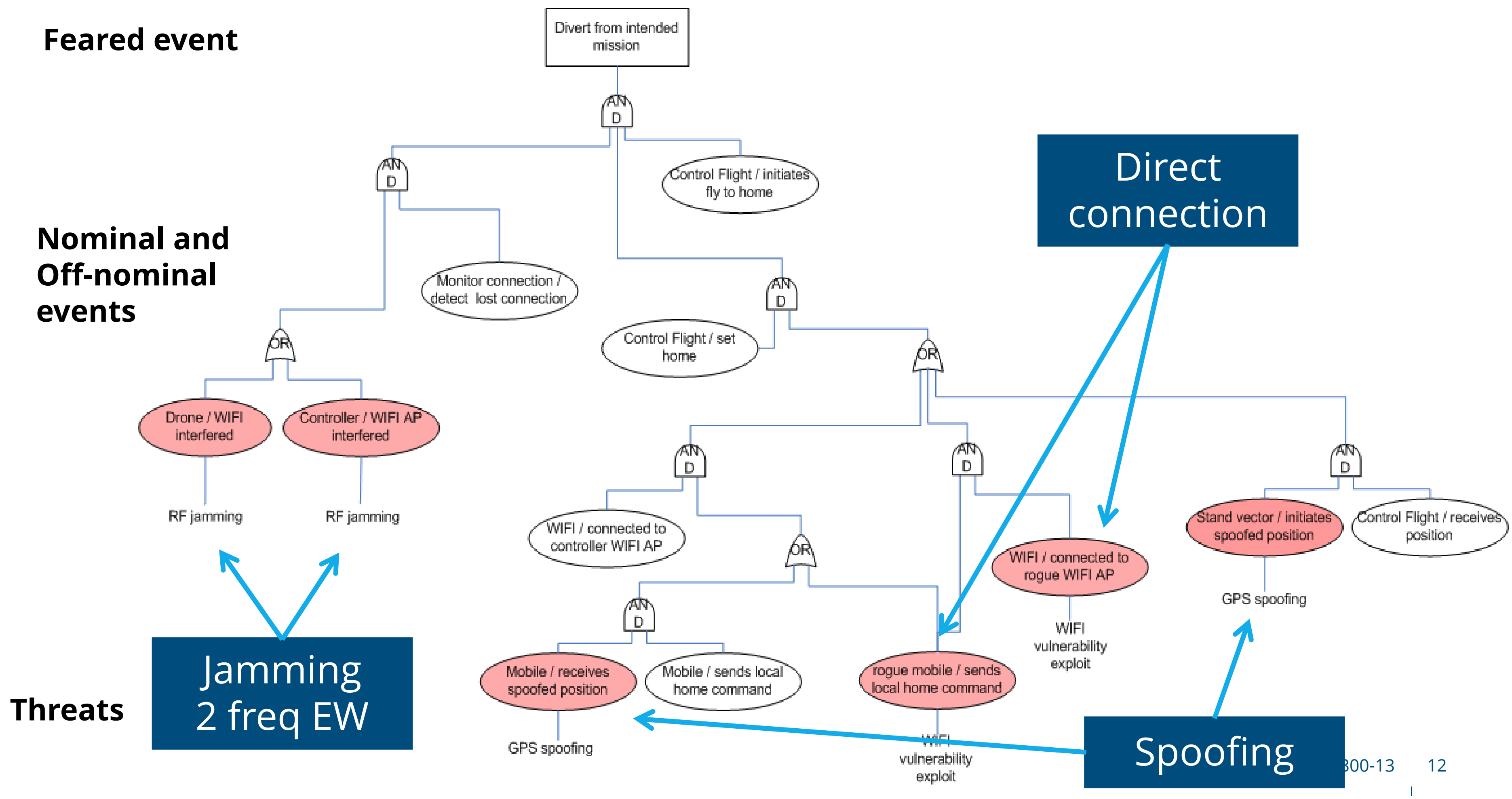




Commercial drone – functional design



Example threat scenario



Likelihood estimation for a given threat (1/2)

A *perpetrator* is defined by its characteristics:

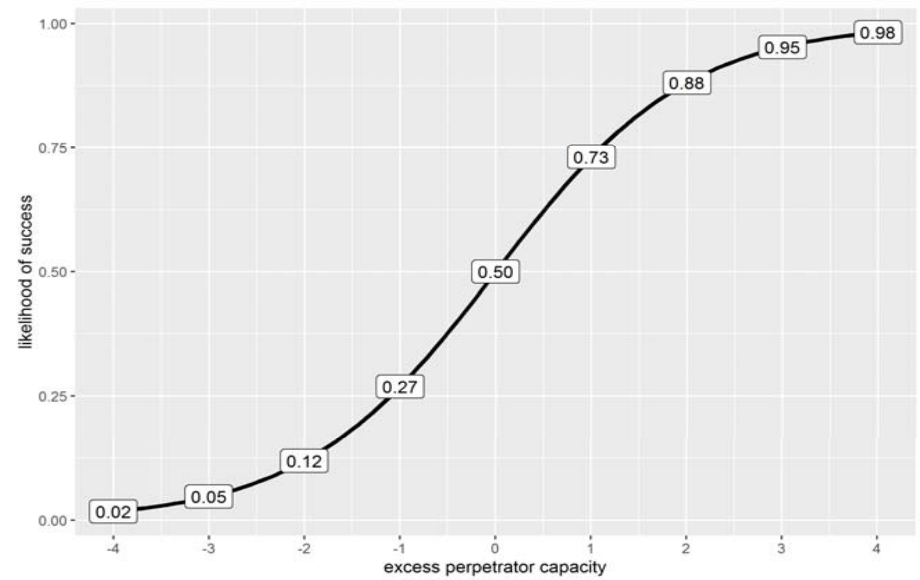
- Expertise
- Knowledge of the target
- Means
  - technical
  - window of opportunity (time needed versus time available)

	… possessed by perpetrator P (capability)	… needed to perform attack A (requirement)
Expertise	$C^P_{\text{expertise}}$	$R^A_{\text{expertise}}$
Knowledge	$C^P_{\text{knowledge}}$	$R^A_{\text{knowledge}}$
Means	C^P_{means}	R^A_{means}

→ *likelihood of perpetrator P succeeding at attack A*

Likelihood estimation (2/3)

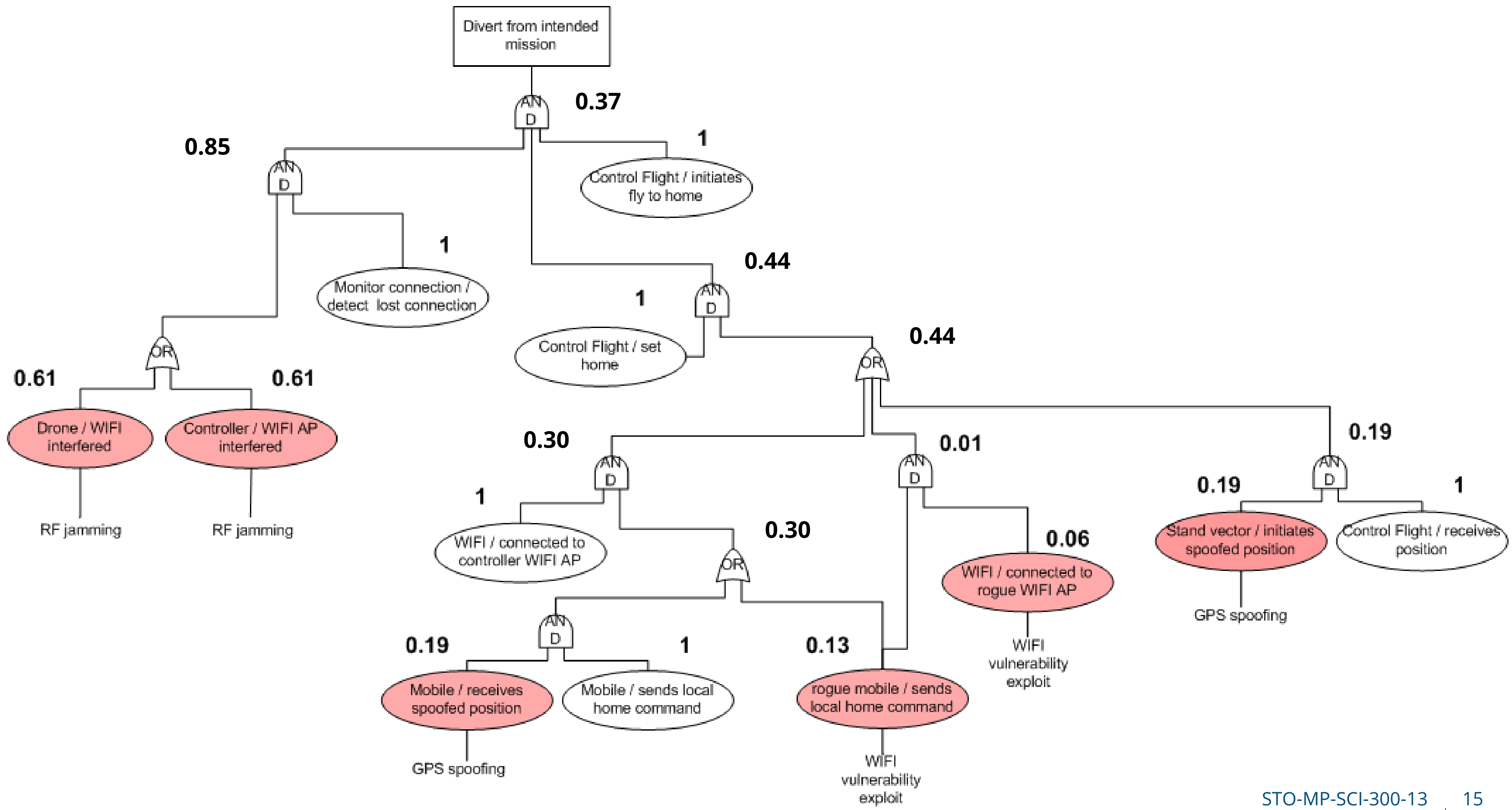
Example:
Feared event: hampering navigation
Perpetrator: a state-sponsored hacker
Threat: GPS spoofing



	Perpetrator capabilities	Attack requirements	Excess perpetrator capability	Likelihood component
Expertise	$C^P_{\text{expertise}} = 5$	$R^A_{\text{expertise}} = 2$	$C^P_{\text{expertise}} - R^A_{\text{expertise}} = +3$	$L^{A\times P}_{\text{expertise}} = 0.95$
Knowledge	$C^P_{\text{knowledge}} = 4$	$R^A_{\text{knowledge}} = 3$	$C^P_{\text{knowledge}} - R^A_{\text{knowledge}} = 1$	$L^{A\times P}_{\text{knowledge}} = 0.73$
Means	$C^P_{\text{means}} = 4$	$R^A_{\text{means}} = 5$	$C^P_{\text{means}} - R^A_{\text{means}} = -1$	$L^{A\times P}_{\text{means}} = 0.27$

$$L^{A|P} = L^{A\,|\,P}_{\text{expertise}} \times L^{A\,|\,P}_{\text{knowledge}} \times L^{A\,|\,P}_{\text{means}} = 0.19$$

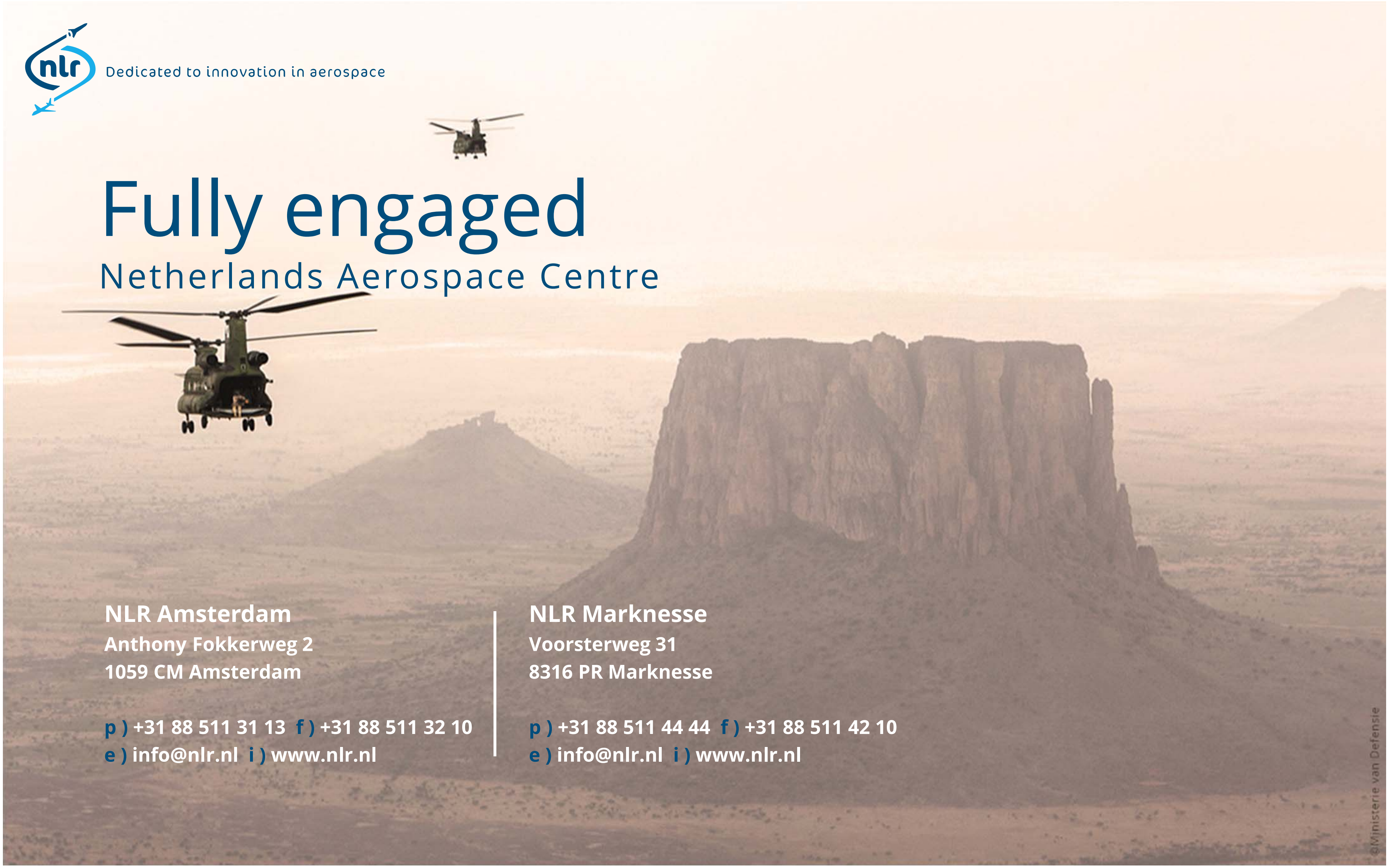
Likelihood estimation, example (3/3)



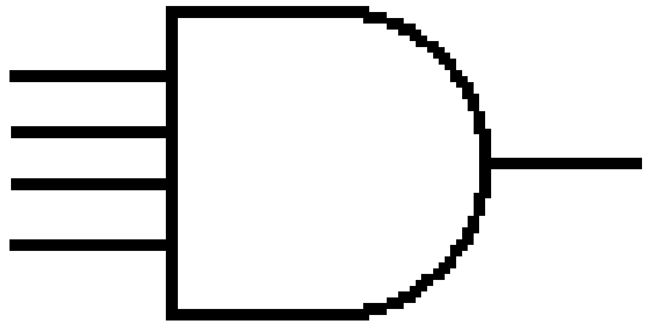
Impact

Per threat scenario ....

		Impact areas				Criteria		
Impact rating	**Flight safety**	**Communication**	**Navigation**	**Surveillance**	**Task execution**	**Damage Human**	**Damage Material**	**Damage Environment**
5 - Catastrophic	High	High	High	Impossible	Complete failure	Fatalities	> 10.000.000	Catastrophic impact
4 - Critical	Some but not all of the HIGH consequences above	Medium-High	Medium-High	Medium-High	Almost complete failure	Multiple severe injuries	> 1.000.000, < 10.000.000	Long term impact
3 - Severe	Medium	Medium	Medium	Medium	Partial failure	Severe injuries	1.000.000	Noticeable impact
2 - Minor	Some but not all of the MEDIUM consequences above	No-Medium	No-Medium	No-Medium	No failure, but additional effort	Minor injuries	> 5000, < 1.000.000	Short term impact
1 - No impact	No	No	No	No	No failure	No injuries	< 5000	Insignificant


nlr
Dedicated to innovation in aerospace
Fully engaged
Netherlands Aerospace Centre
NLR Amsterdam
Anthony Fokkerweg 2
1059 CM Amsterdam
p) +31 88 511 31 13 f) +31 88 511 32 10
e) info@nlr.nl i) www.nlr.nl
NLR Marknesse
Voorsterweg 31
8316 PR Marknesse
p) +31 88 511 44 44 f) +31 88 511 42 10
e) info@nlr.nl i) www.nlr.nl
©Ministerie van Defensie

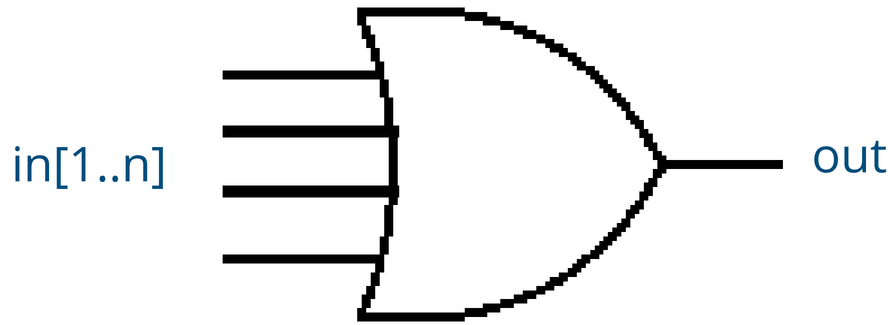
AND result



Out = in[1] x in[2] x ……. x in[n]

Out = $\prod_{1}^{n} in[i]$

OR result



Out = 1.0 - (1.0 - in[1]) x (1.0 - in[2]) x .... x (1.0 - in[n])

Out = 1.0 – $\prod_{1}^{n}(1.0 - in[i])$

Assumption: inputs are independent from each other, otherwise calculation becomes more complicated