RISKEE

A Risk-Tree Based Method for Assessing Risk in Cyber Security

Michael Krisper
Graz University of Technology

26th EuroSPI²
Sept. 2019, Edinburgh

The Old Packhorse Bridge, Carrbridge, Aviemore, Schottland
Oldest Stone Bridge in Schottland. 1717, took 6 month to build, cost £100

Risk Assessment in Cyber-Security

What is the Problem?

- **Cyber-security incidents inflict tremendous costs.**
  Especially private sector, infrastructure, finance, health, and government are common and profitable targets for hackers.

- Cyber-security incidents are **very hard to predict.**
  (=**huge uncertainty** in predictions)

- Commonly used qualitative methods **neglect uncertainty or do not quantify risk** and may impose a **wrong sense of security** and safety.

- This makes it very **difficult** for managers to **decide** for the appropriate **mitigation and hardening strategies**.

The Risk of Cyber-Security

Austrian People's Party calls alleged hack an 'attack on democracy'

News comes ahead of snap election and after revelation party broke spending laws

Fri, Sep 6, 2019, 18:41

https://www.irishtimes.com/news/world/europe/austrian-people-s-party-calls-alleged-hack-an-attack-on-democracy-1.4010308

A new organization will fall victim to ransomware every **14 seconds** in 2019, and every 11 seconds by 2021.

https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

We are losing the cyber war… We have to do something. (Larry Ellison, Oracle)

https://www.computing.co.uk/ctg/news/3018543/-we-are-losing-the-cyber-war-says-oracles-larry-ellison-as-he-introduces-automated-security

Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021 https://cybersecurityventures.com/cybersecurity-market-report/

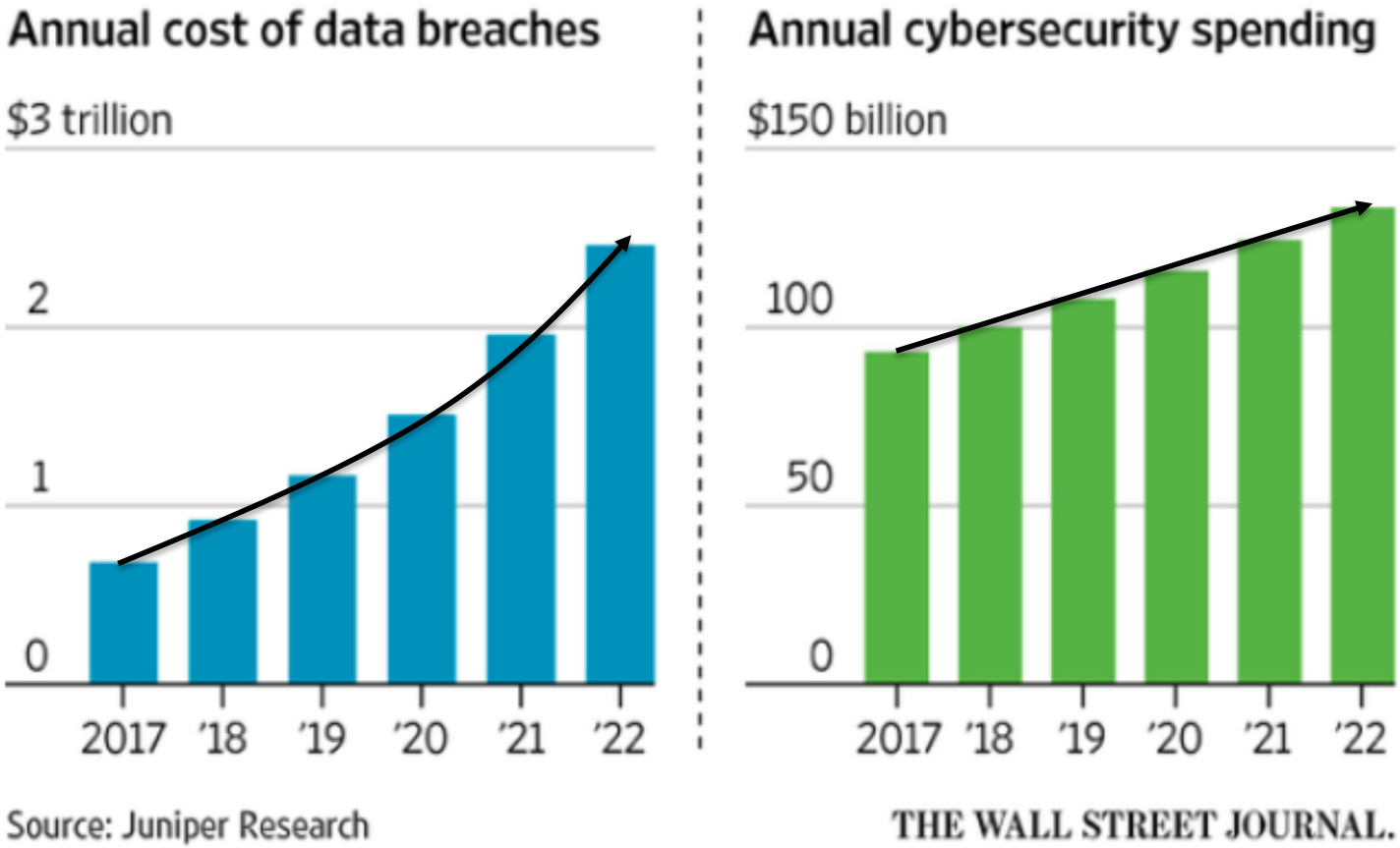
An overwhelming number of IT security professionals (85%) see a cyberattack on critical infrastructure happening in the next five years

https://www.prnewswire.com/news-releases/the-big-cyber-attack-is-coming-85-of-it-security-pros-tell-pwnie-express-300649091.html

Ransomware costs businesses more than $75 billion per year.

https://www.datto.com/news/american-small-businesses-lose-an-estimated-75-billion-a-year-to-ransomware

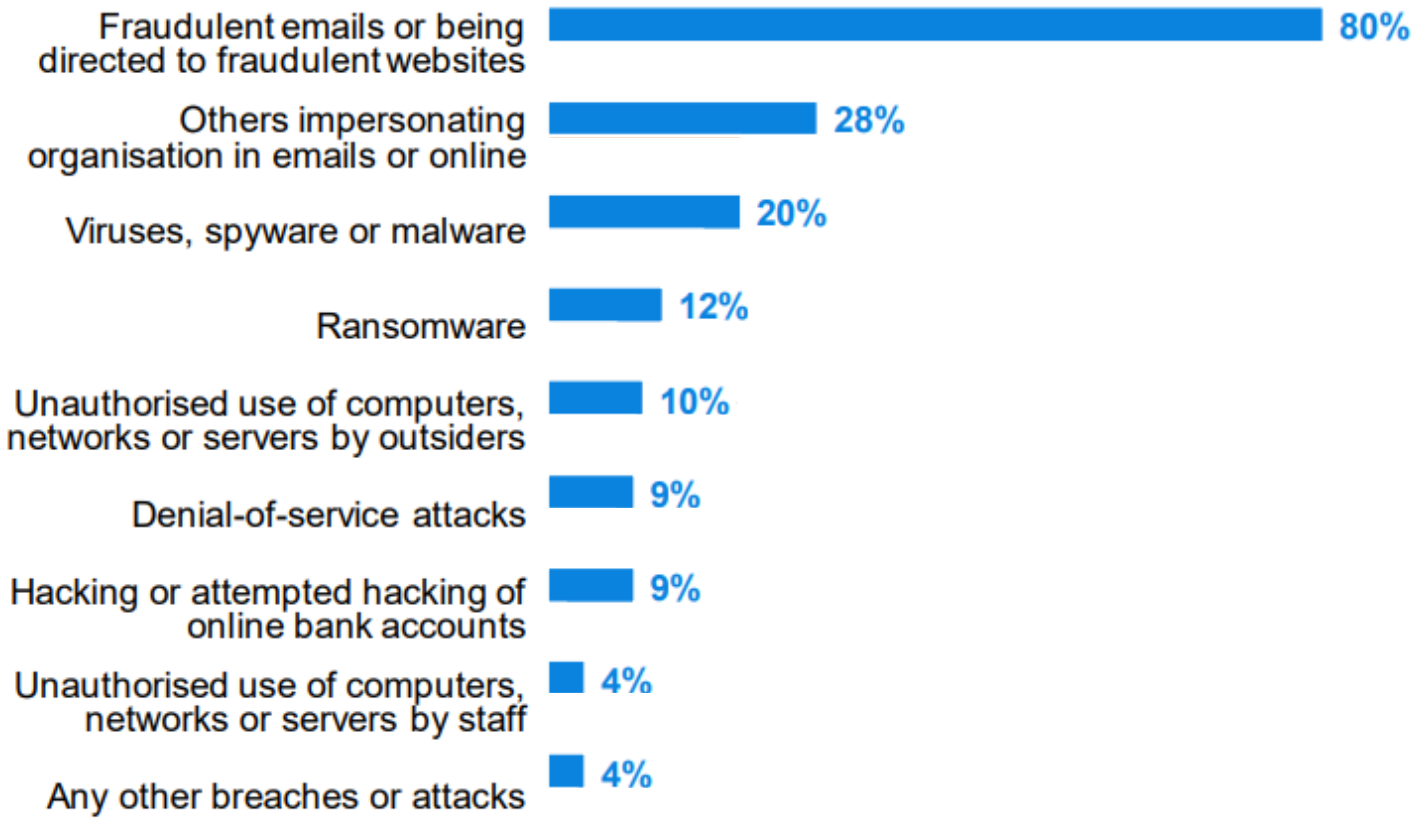
The Cost of Cyber Security



https://www.wsj.com/articles/the-evolution-of-a-cybersecurity-firm-1494986640

What kinds of attacks happen?

Q. Have any of the following happened to your organisation in the last 12 months?

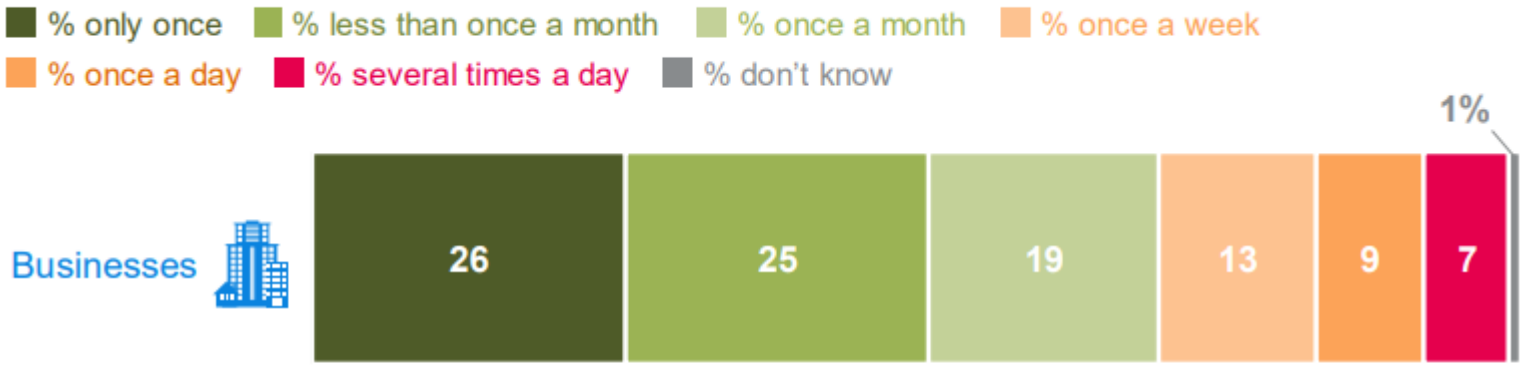


Bases: 637 businesses that identified a breach or attack in the last 12 months; 192 charities

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf]

How often?

Q. Approximately how often in the last 12 months did you experience cyber security breaches or attacks?

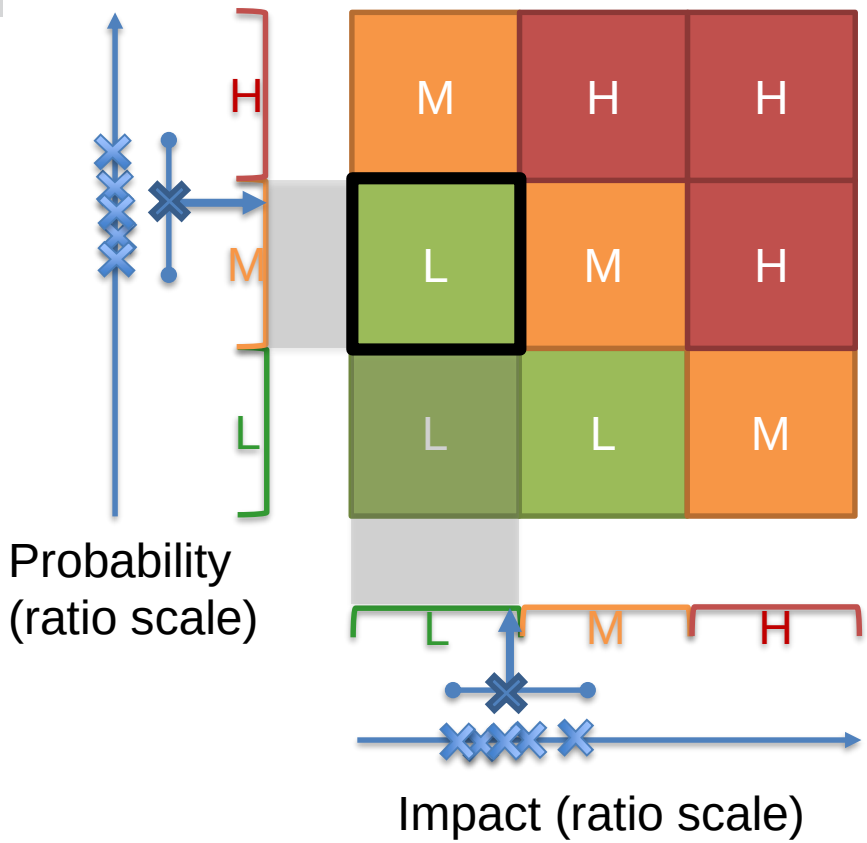


Bases: 637 businesses that identified a breach or attack in the last 12 months; 192 charities

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf]

Problems?

Problem: Ordinal Scales and Risk Matrices



Low Risk:
- Diagnostic Coverage > 90%
- No fail-recovery needed
- No rigorous testing methods needed

10$

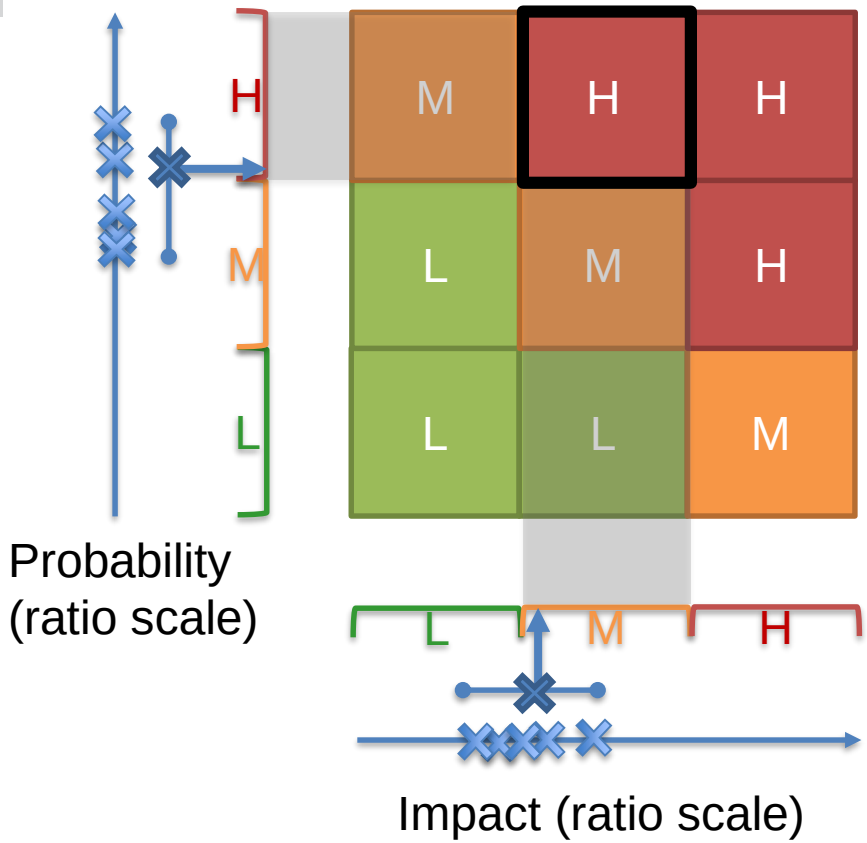
Medium Risk:
- Diagnostic Coverage > 99%
- Degraded fail-recovery required
- Some testing methods required

50$

High Risk:
- Diagnostic Coverage > 99.9%
- Full fail-over / fail-safe
- Many rigorous testing methods required

100$

Problem: Ordinal Scales and Risk Matrices



Low Risk:
- Diagnostic Coverage > 90%
- No fail-recovery needed
- No rigorous testing methods needed

10$

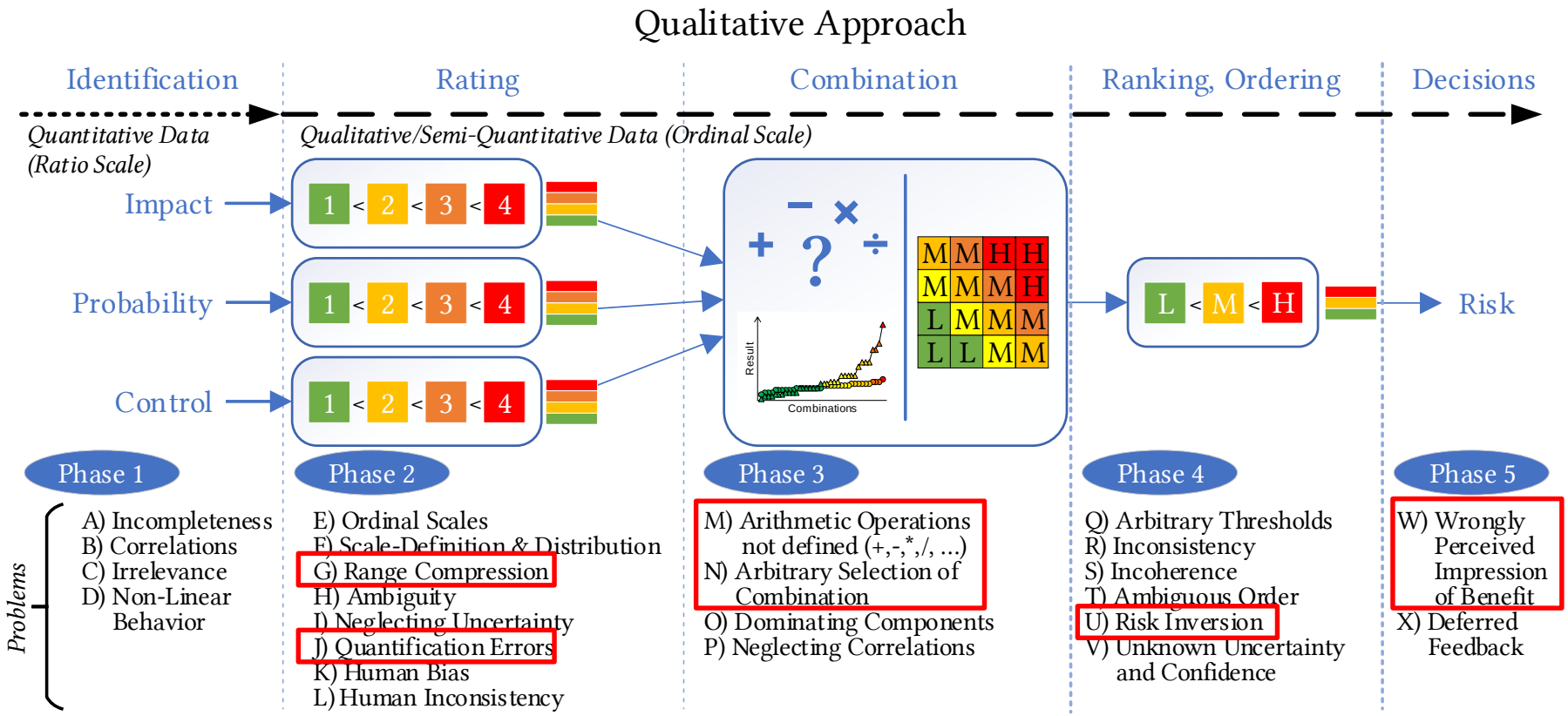
Medium Risk:
- Diagnostic Coverage > 99%
- Degraded fail-recovery required
- Some testing methods required

50$

High Risk:
- Diagnostic Coverage > 99.9%
- Full fail-over / fail-safe
- Many rigorous testing methods required

100$

Problem: Existing Risk Methods use Ordinal Scales & Risk Matrices



Cox, Anthony Louis. 2008. “What’s Wrong with Risk Matrices?” *Risk Analysis* 28 (2): 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x.
Hubbard, D., and D. Evans. 2010. “Problems with Scoring Methods and Ordinal Scales in Risk Assessment.” *IBM Journal of Research and Development,* https://doi.org/10.1147/JRD.2010.2042914.
Krisper, Michael, et. al. 2019. “Pitfalls, Fallacies, and Other Problems in Risk Matrices Using Ordinal Scales”

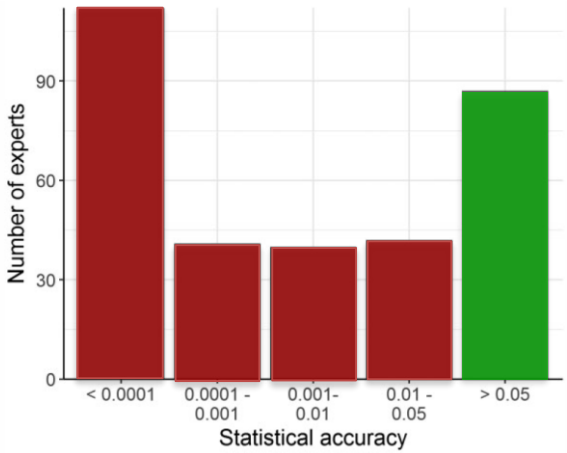
Predictions difficult? What about Expert Judgement?

Expert Elicitation: Using the Classical Model to Validate Experts' Judgments

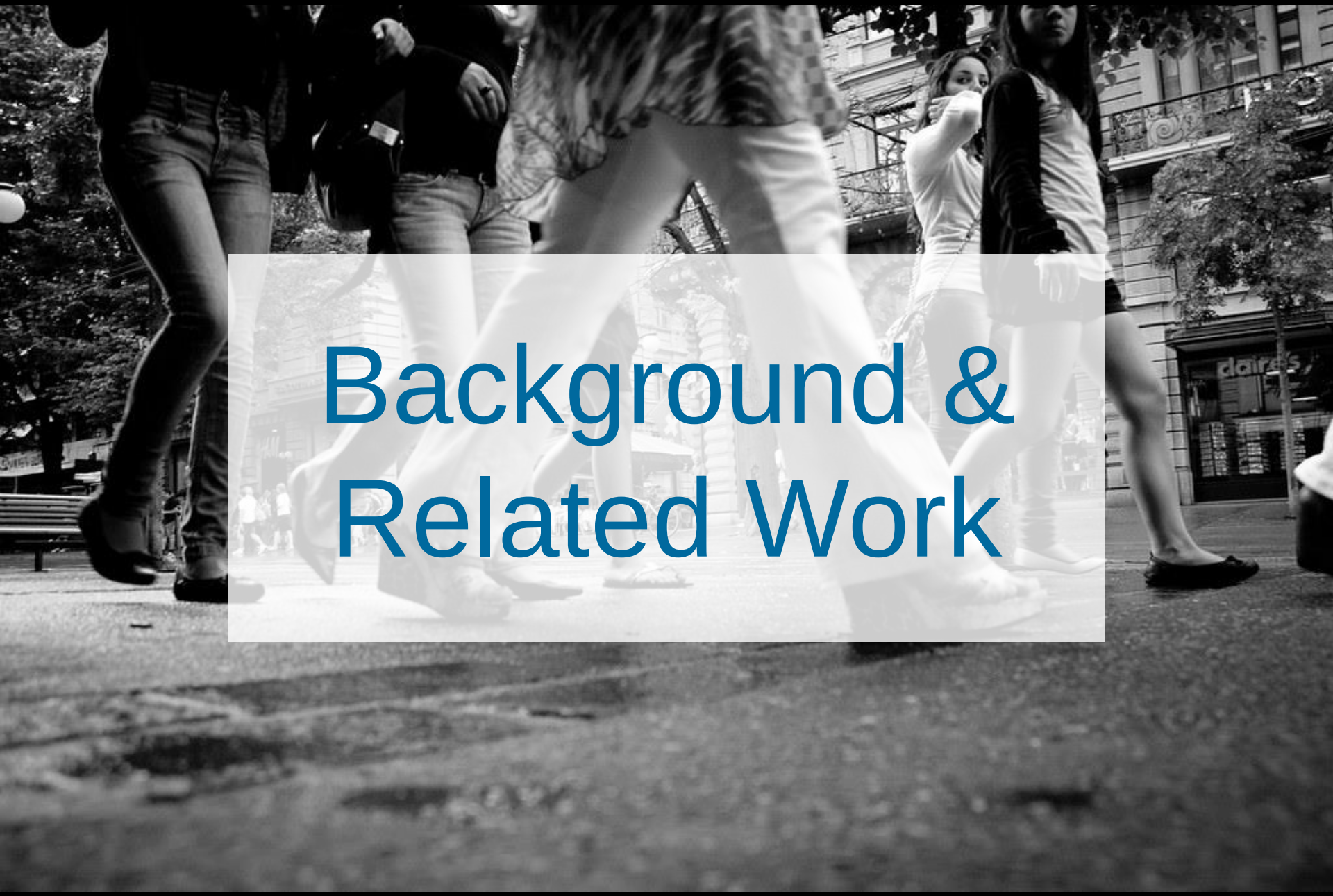
Abigail R. Colson* and Roger M. Cooke†

- Meta-Study over 33 Studies with Expert Judgements between 2006 and 2015
  (323 experts, different domains)

- *Result:* ~2/3 of expert judgements are inaccurate should be rejected.



Colson, Abigail R, and Roger M Cooke. 2018. "Expert Elicitation: Using the Classical Model to Validate Experts' Judgments." *Review of Environmental Economics and Policy* 12 (1): 113–32. https://doi.org/10.1093/reep/rex022.
Cooke, Roger M., *The Confidence Trap: Dysfunctional Dialogues about Climate,* Invited Talk, ETH Zürich, Dec 2018]

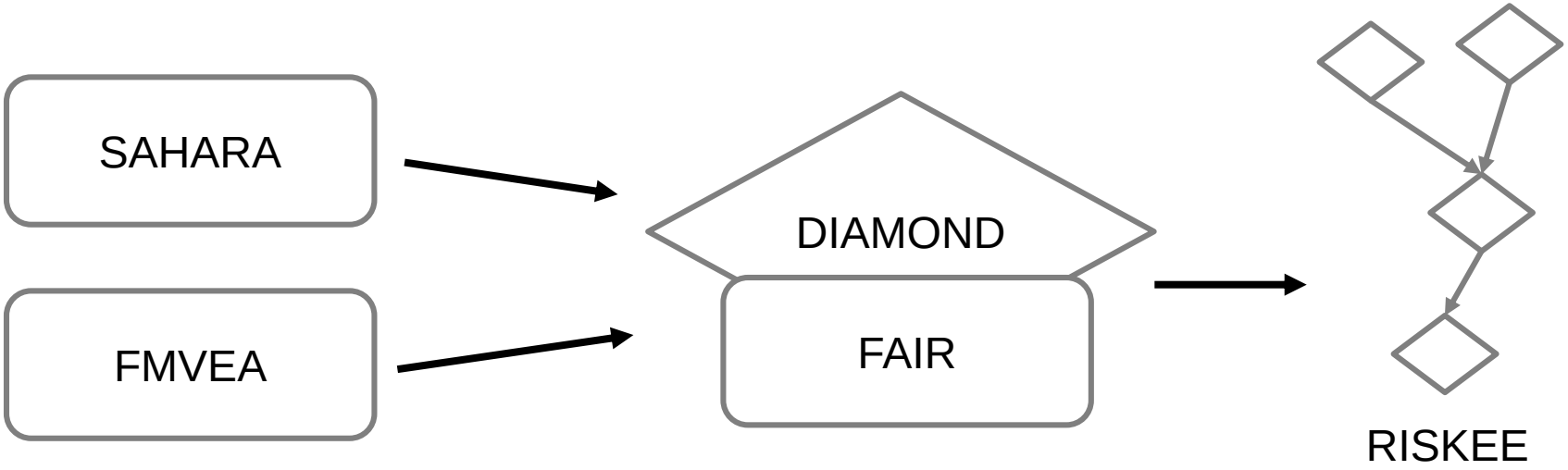


Background & Related Work

Integrated Quantitative Security and Safety Risk Assessment

Idea:

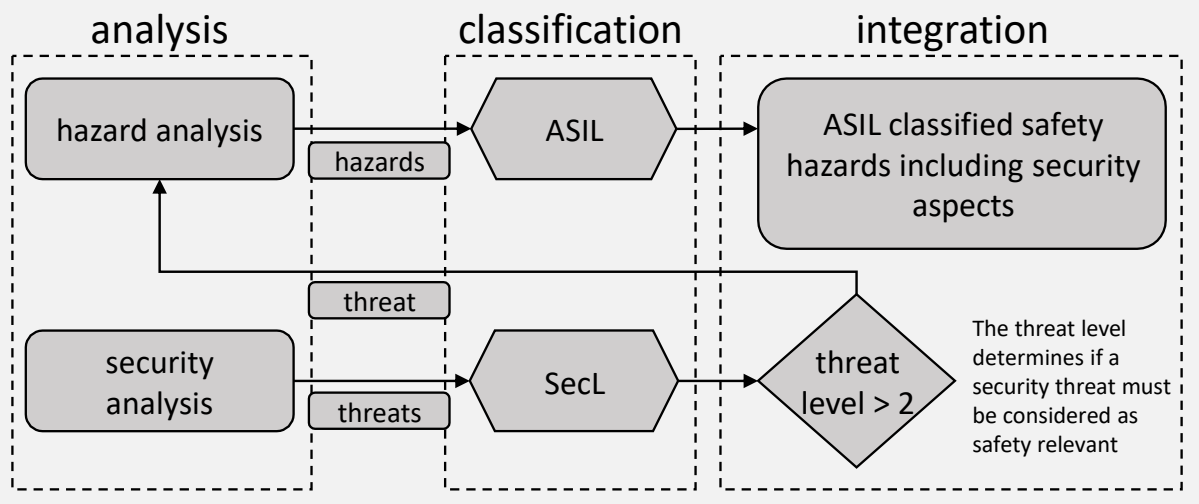
Map ordinal ratings and attributes from existing methods (SAHARA, FMVEA) to quantitative information for risk assessment with RISKEE.



Dobaj, Jürgen, Christoph Schmittner, Michael Krisper, and Georg Macher. 2019. “Towards Integrated Quantitative Security and Safety Risk Assessment.” In *Computer Safety, Reliability, and Security*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-26250-1_8.

SAHARA

Security Extension to HARA



Required Resources 'R'	Required Know-How 'K'	Threat Level 'T' 0	1	2	3
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

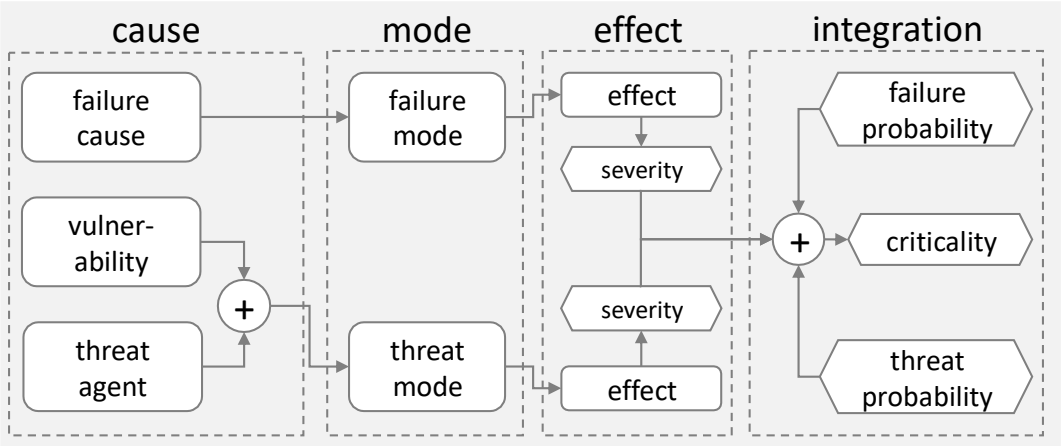
R: Resources $[0-3]$
K: Know−How $[0-2]$
T: Threat Criticality $[0-3]$

$$SecL = \begin{cases} 4 & \text{if } 5-K-R+T \geq 7 \\ 3 & \text{if } 5-K-R+T = 6 \\ 2 & \text{if } 5-K-R+T = 5 \\ 1 & \text{if } 5-K-R+T = 4 \\ 1 & \text{if } T=3, K=2, R=3 \\ 0 & \text{if } 5-K-R+T < 4 \ or \ T=0 \end{cases}$$

Macher, Georg, et al. 2016. “A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context.” In *Computer Safety, Reliability, and Security*, Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-45477-1_11.
Macher, Georg, et al., 2015. “SAHARA: A Security-Aware Hazard and Risk Analysis Method.”, *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, 2015. https://doi.org/10.7873/DATE.2015.0622.

FMVEA

Security Extension to FMEA



$Motivation\ [1-3]$
$+\ Capabilities\ [1-3]$

System Susceptibility					
6	8	9	10	11	12
5	7	8	9	10	11
4	6	7	8	9	10
3	5	6	7	8	9
2	4	5	6	7	8
	2	3	4	5	6

Threat properties

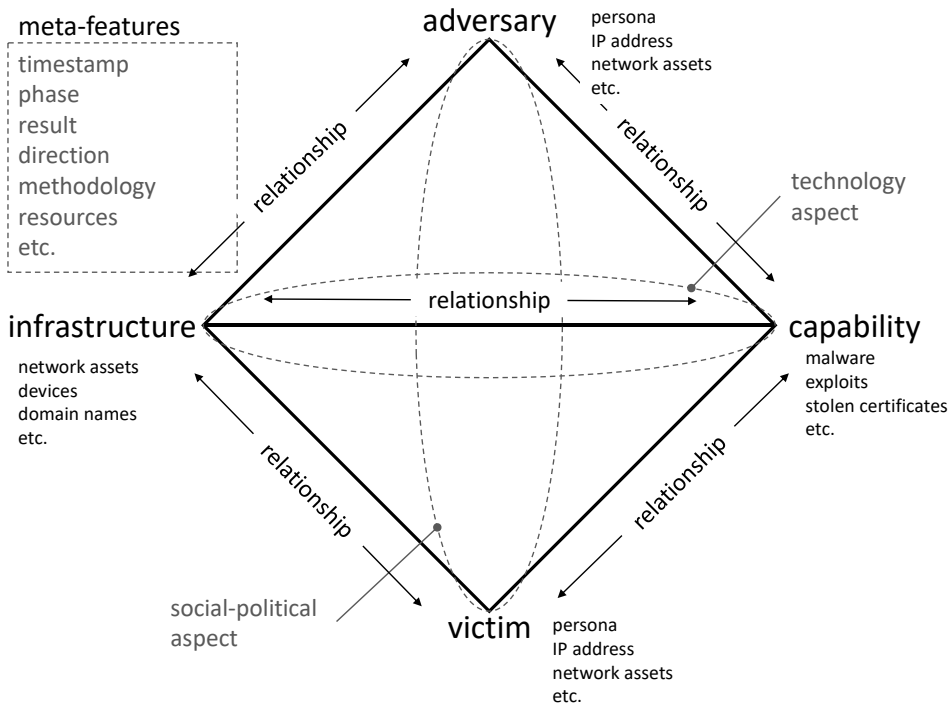
$Reachability\ [1-3]$
$+\ Unusualness\ [1-3]$

$$\boldsymbol{Attack\ Probability}[\mathbf{4-12}]$$
$$= System\ Susceptibility[2-6]$$
$$+\ Threat\ Properties[2-6]$$
$$= M + C + R + U$$

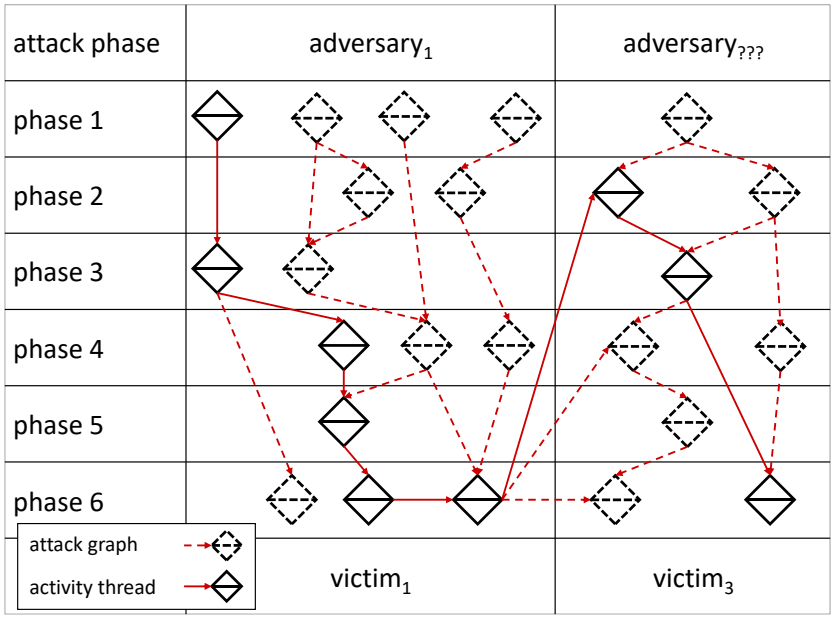
Schmittner, Christoph, Thomas Gruber, Peter Puschner, and Erwin Schoitsch. 2014. “Security Application of Failure Mode and Effect Analysis (FMEA).” In *Computer Safety, Reliability, and Security*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-10506-2_21.

Diamond Model

Diamond = Model of an Attack

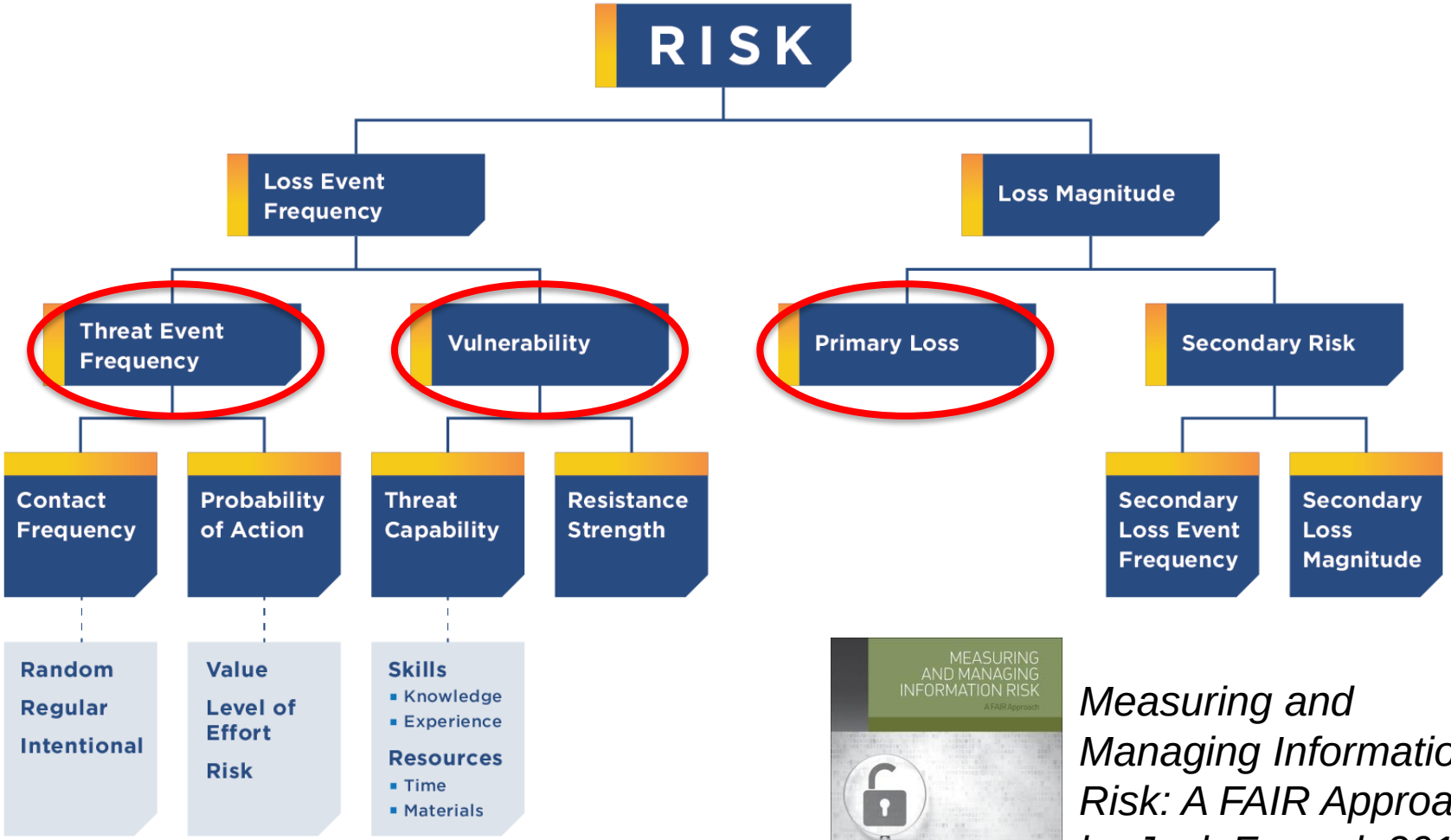


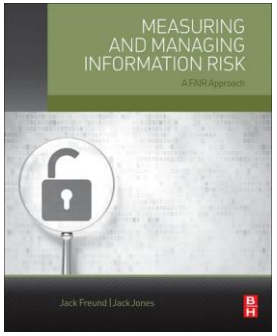
Attack Trees / Kill Chain



Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. 2013. “The Diamond Model of Intrusion Analysis.” Center for Cyber Intelligence Analysis and Threat Research Hanover MD.

Factor Analysis of Information Risk (FAIR)



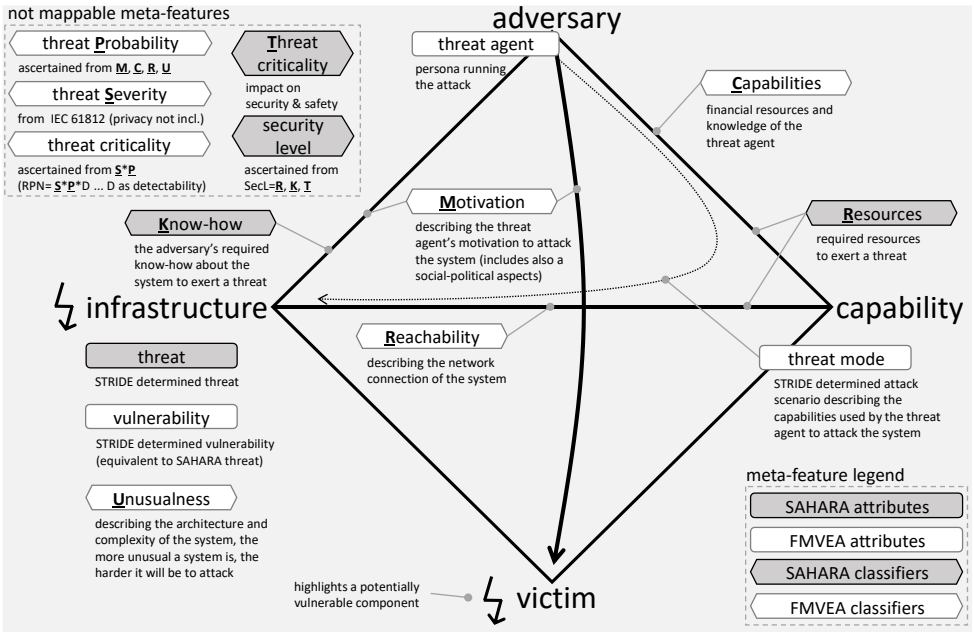


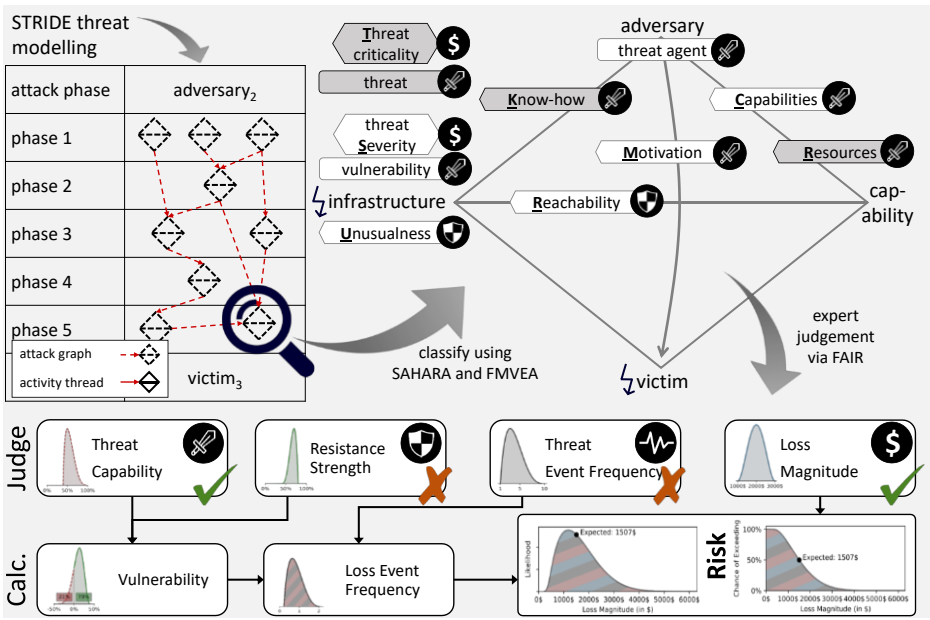
Measuring and Managing Information Risk: A FAIR Approach by Jack Freund, 2015

[Freund, Jack. 2015. *Measuring and Managing Information Risk: A FAIR Approach*.]
[The Open Group. 2013a. “Risk Analysis (O-RA).”][The Open Group. 2013b. “Risk Taxonomy (O-RT) 2.0.”]

Integrated Quantitative Security and Safety Risk Assessment

Map ordinal ratings and attributes from existing methods (SAHARA, FMVEA) to quantitative information for risk assessment with RISKEE.





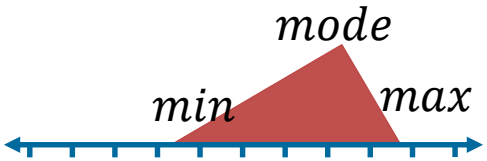
Dobaj, Jürgen, Christoph Schmittner, Michael Krisper, and Georg Macher. 2019. "Towards Integrated Quantitative Security and Safety Risk Assessment." In *Computer Safety, Reliability, and Security*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-26250-1_8.

Estimates with Distributions

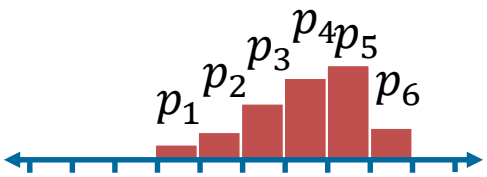
Single-Point Estimate

Range (Interval)

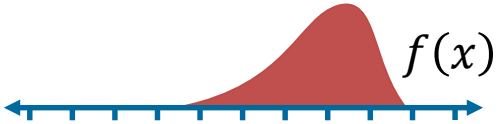
Three-Point Estimate



Histograms



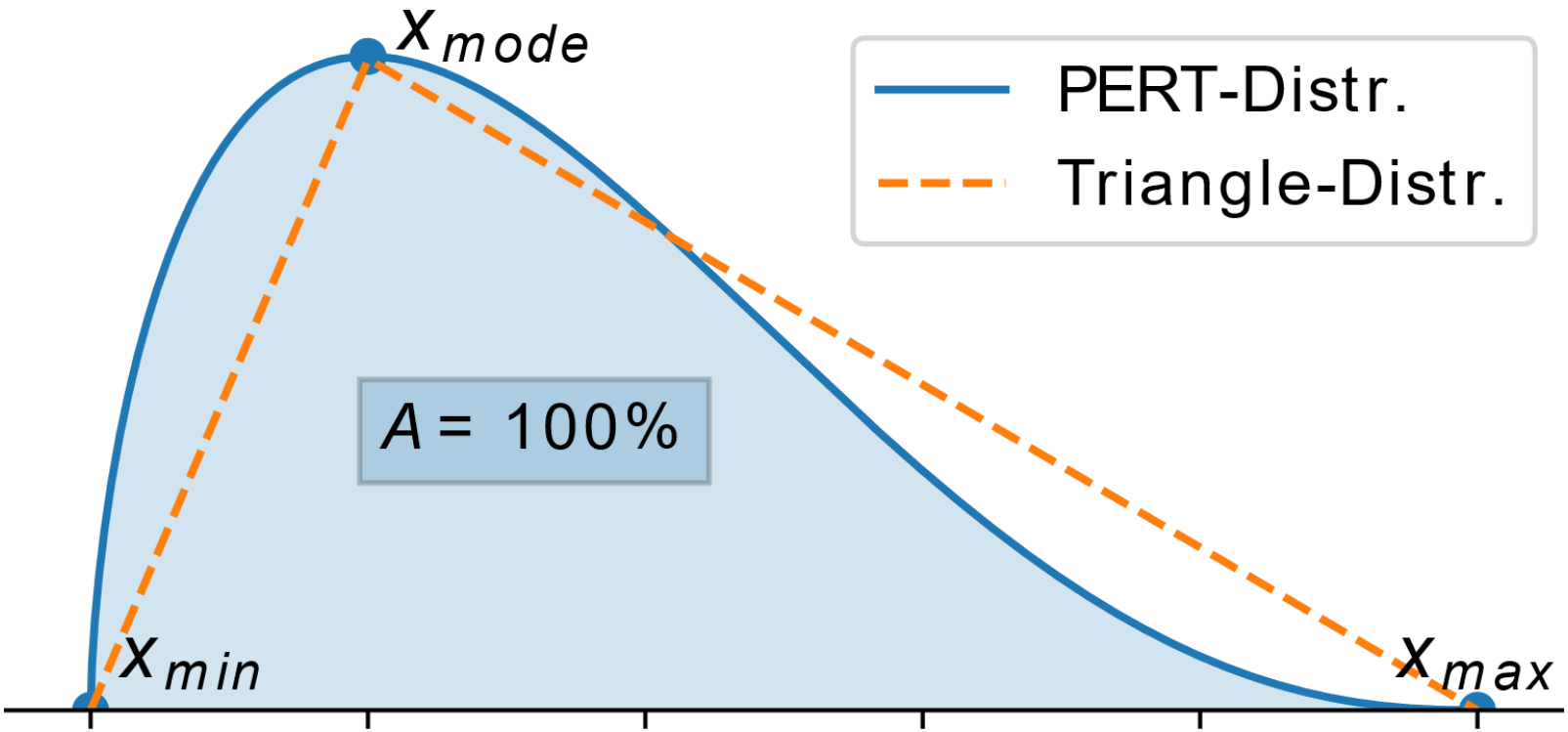
Probability Density Functions



$f(x) = \mathrm{Beta}(\alpha, \beta)$

PERT

A Smooth Limited Three-Point Estimate Probability Function



The (modified) PERT Distribution

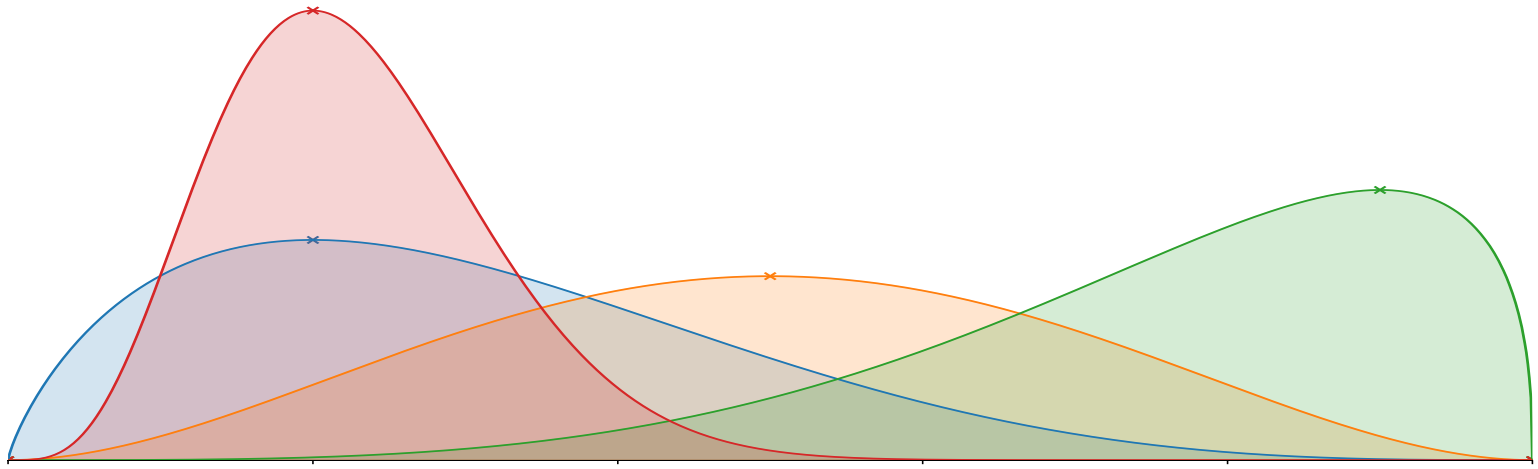
4 Parameters: min, mode, max, confidence

$$\mathrm{PERT}(x; x_{min}, x_{mode}, x_{max}, \lambda) = \frac{(x - x_{min})^{\alpha}(x_{max} - x)^{\beta}}{\mathrm{B}(1+\alpha, 1+\beta)(x_{max} - x_{min})^{\alpha+\beta+1}}$$

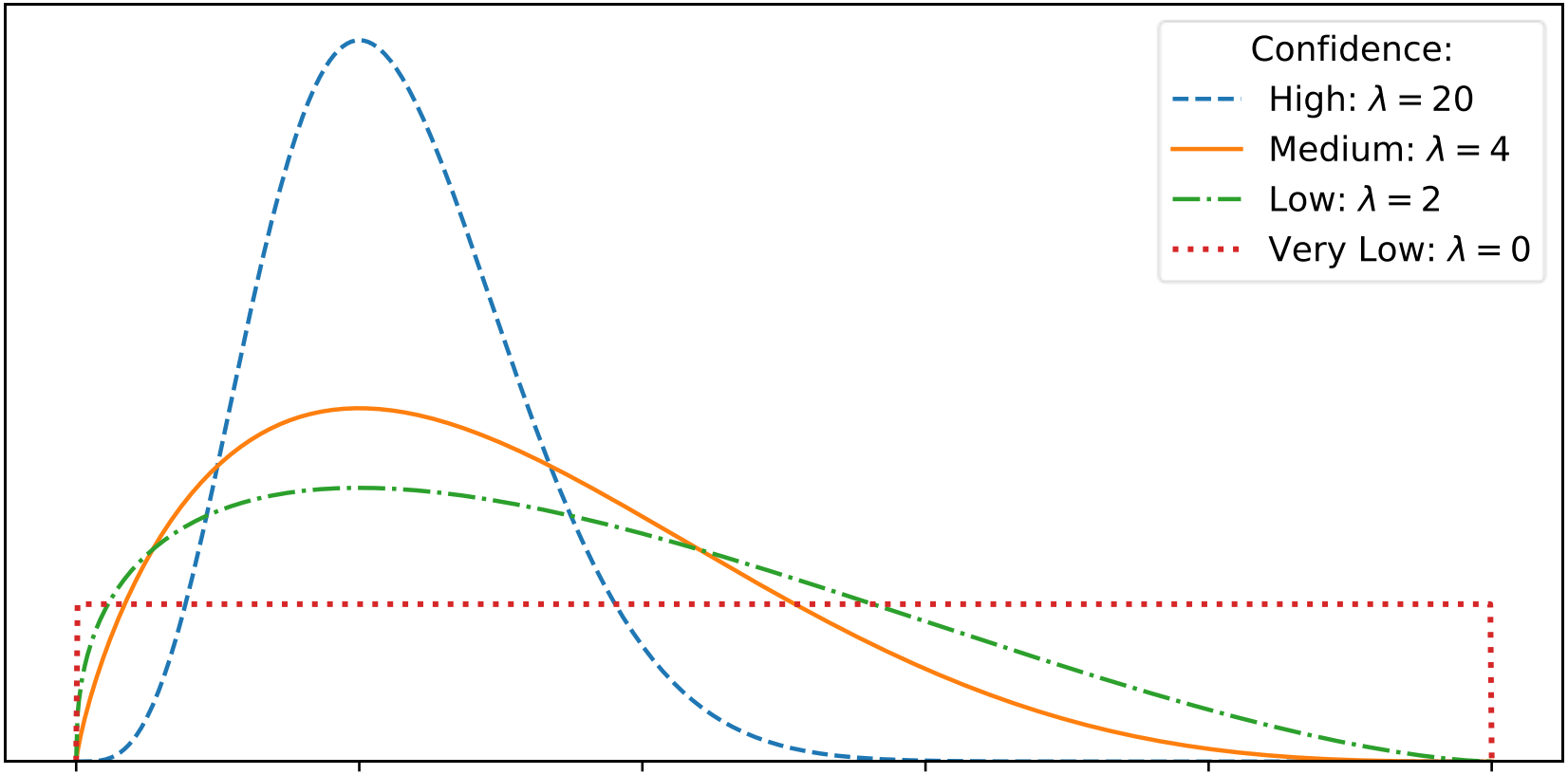
$$\alpha = \frac{\lambda(x_{mode} - x_{min})}{x_{max}}$$

$$\beta = \frac{\lambda(x_{max} - x_{mode})}{x_{max} - x_{min}}$$

$$\mathrm{B}(u, v) = \frac{\Gamma(u)\Gamma(v)}{\Gamma(u+v)}$$



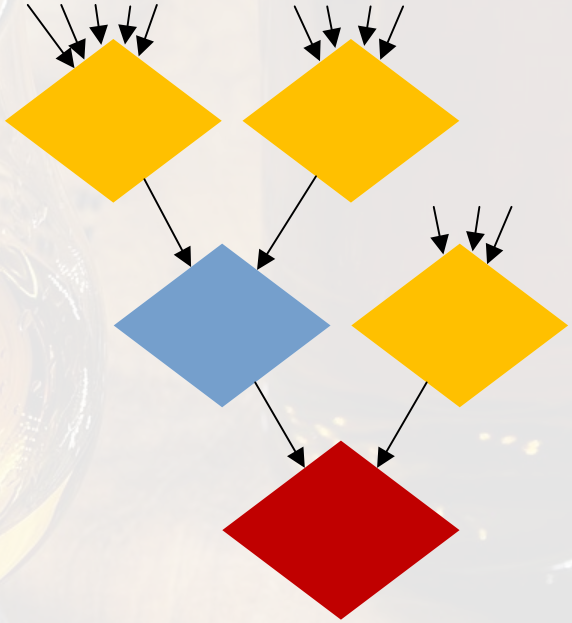
PERT Distribution: Confidence λ
How confident are we in x_{mode}?



Covered so far…

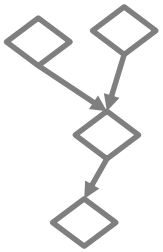
- Risk and Costs in Cyber-Security
- Problems with Established Methods & Risk Matrices
- SAHARA, FMVEA
- Diamond, FAIR
- Probability Distributions, PERT

RISKEE

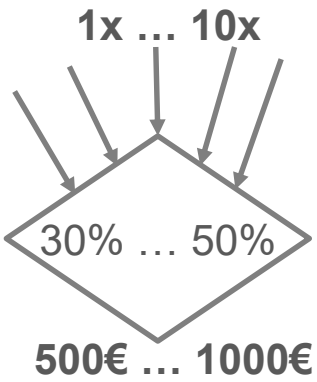


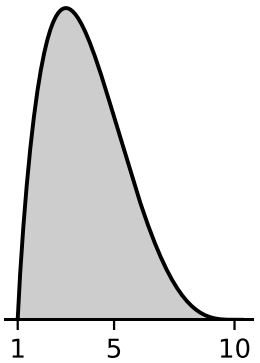
RISKEE – A Risk-Tree Based Method for Assessing Risks

1. Model the attack tree



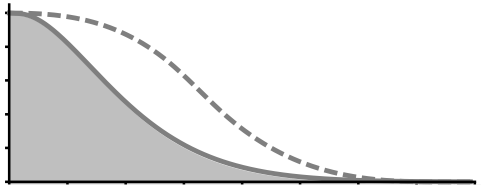
2. Estimate risk attributes
   - Frequency
   - Probability
   - Impact



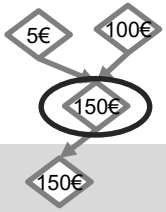


3. Calculate Risk and Propagate Uncertainty

4. Evaluate Loss Exceedance Curve



5. Analyse Risk-Tree



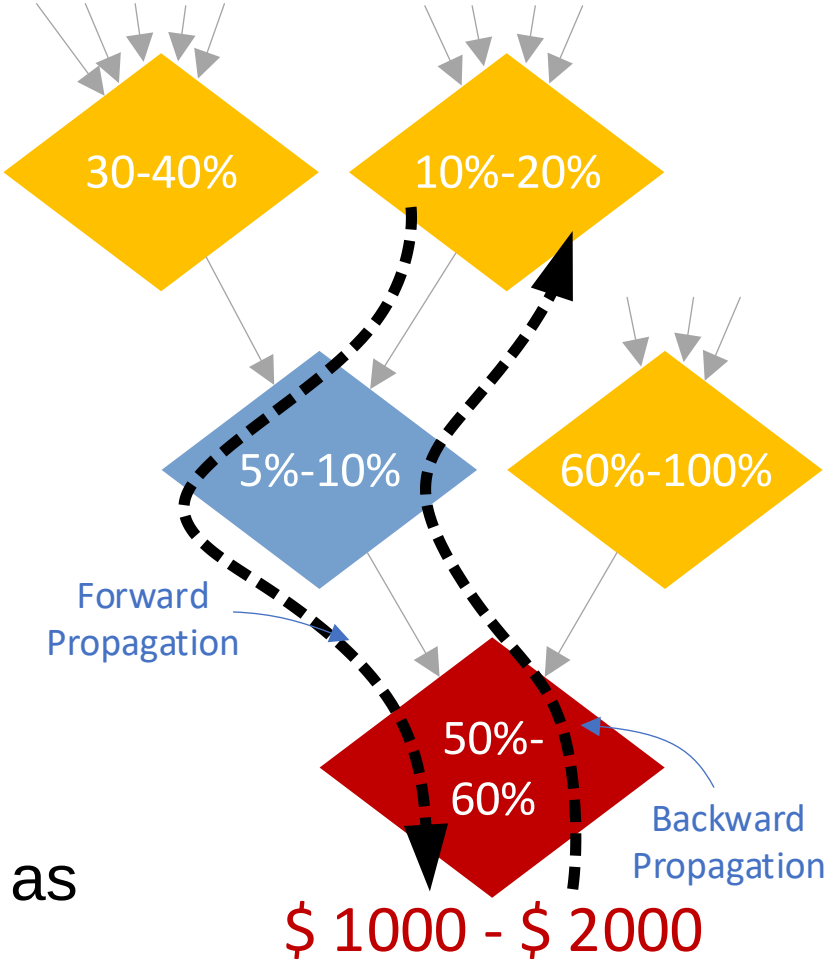
RISKEE – A Risk-Tree Based Method for Assessing Risks

Entry Level Nodes
Attack Surface with ***Attack Frequency***

Intermediate Nodes
Attack Path with ***Vulnerability***

End Nodes
Goals with ***Impact***

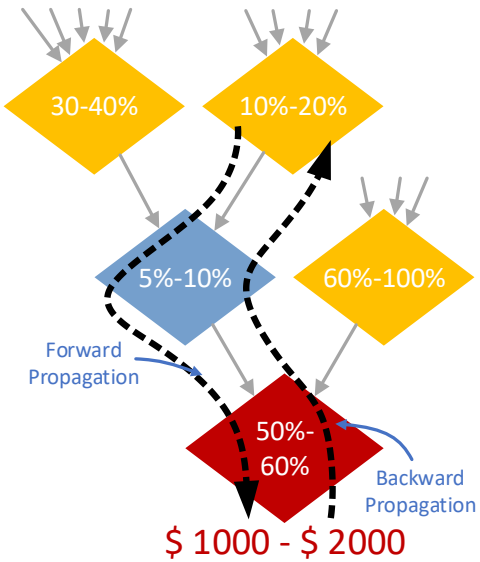
All risk attributes are estimated as probability distributions.



RISKEE – A Risk-Tree Based Method for Assessing Risks

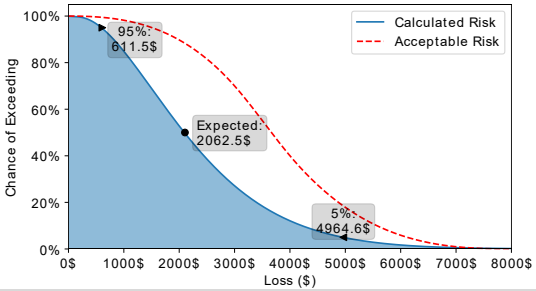
<u>Input:</u>

- Attack Tree/Graph
- Assessment of risk attributes:
  - ***Frequency*** of attacks: [min, mode, max] / year
  - ***Vulnerability*** of nodes: [min%, mode%, max%]
  - ***Impact*** in case of breach: [min€, mode€, max€]



<u>Calculation:</u>

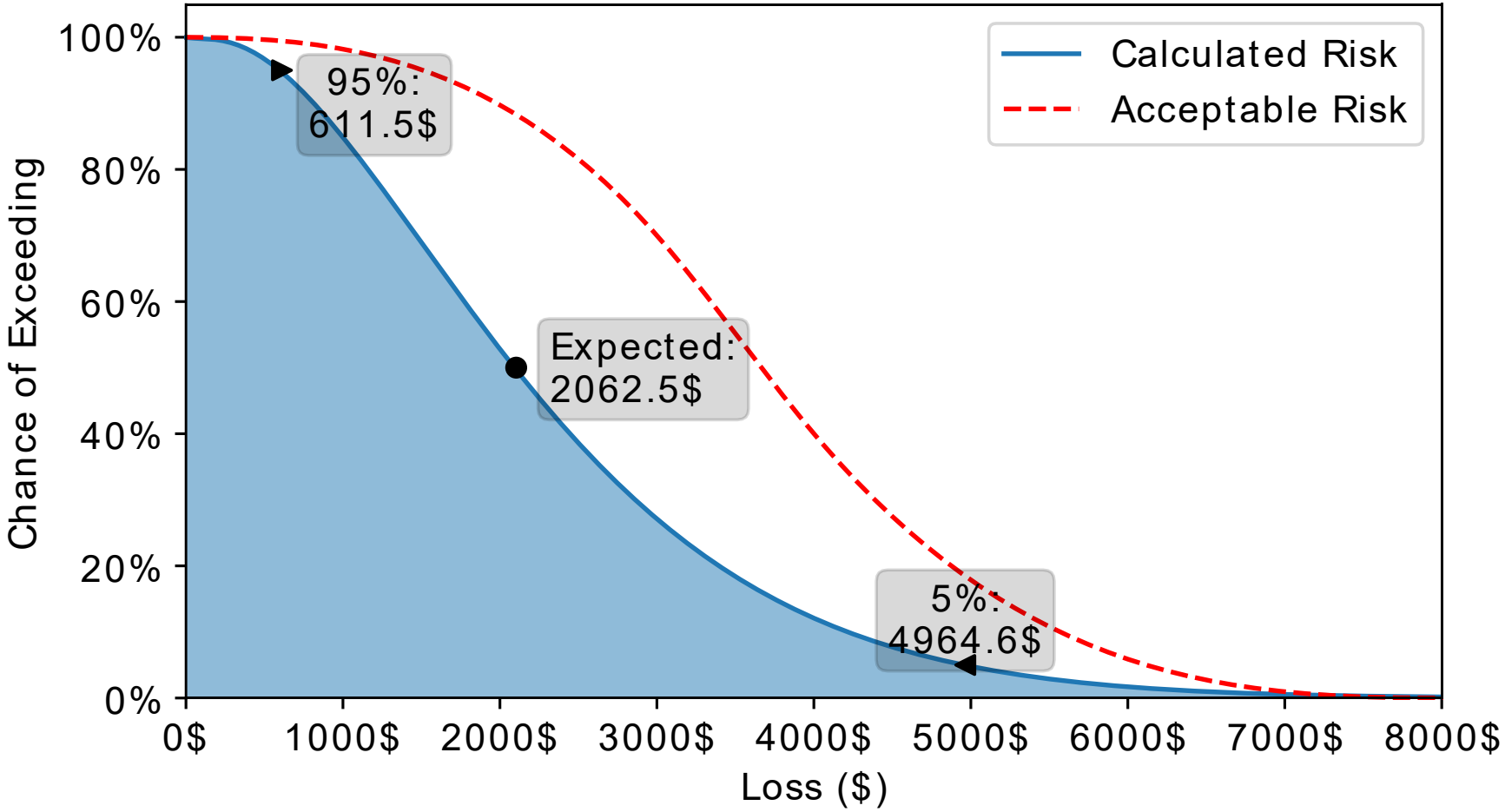
1. *Forward propagation* along all possible paths
2. *Calculation* and summation of risk
3. *Backward propagation* of risk along paths

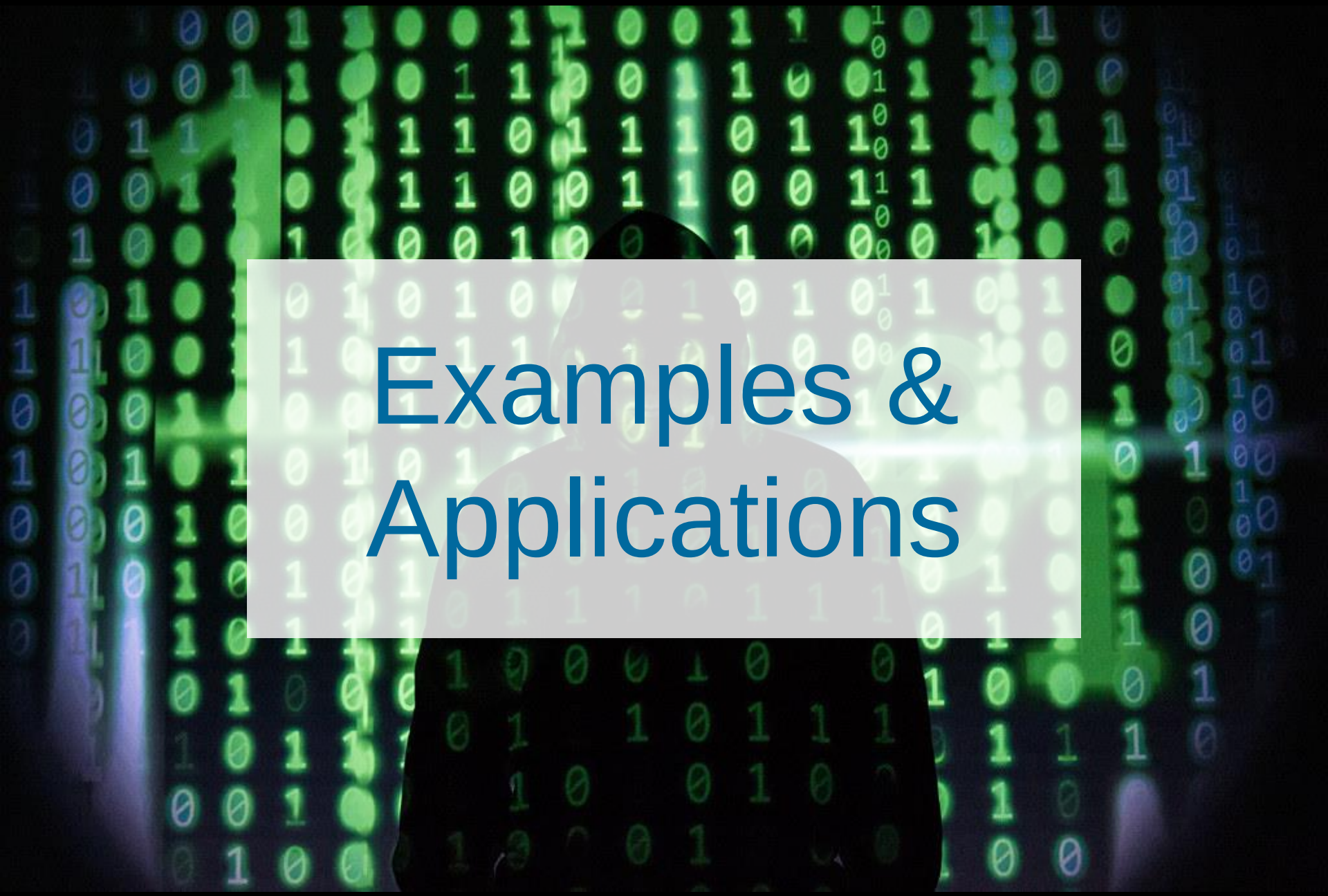


<u>Output:</u>

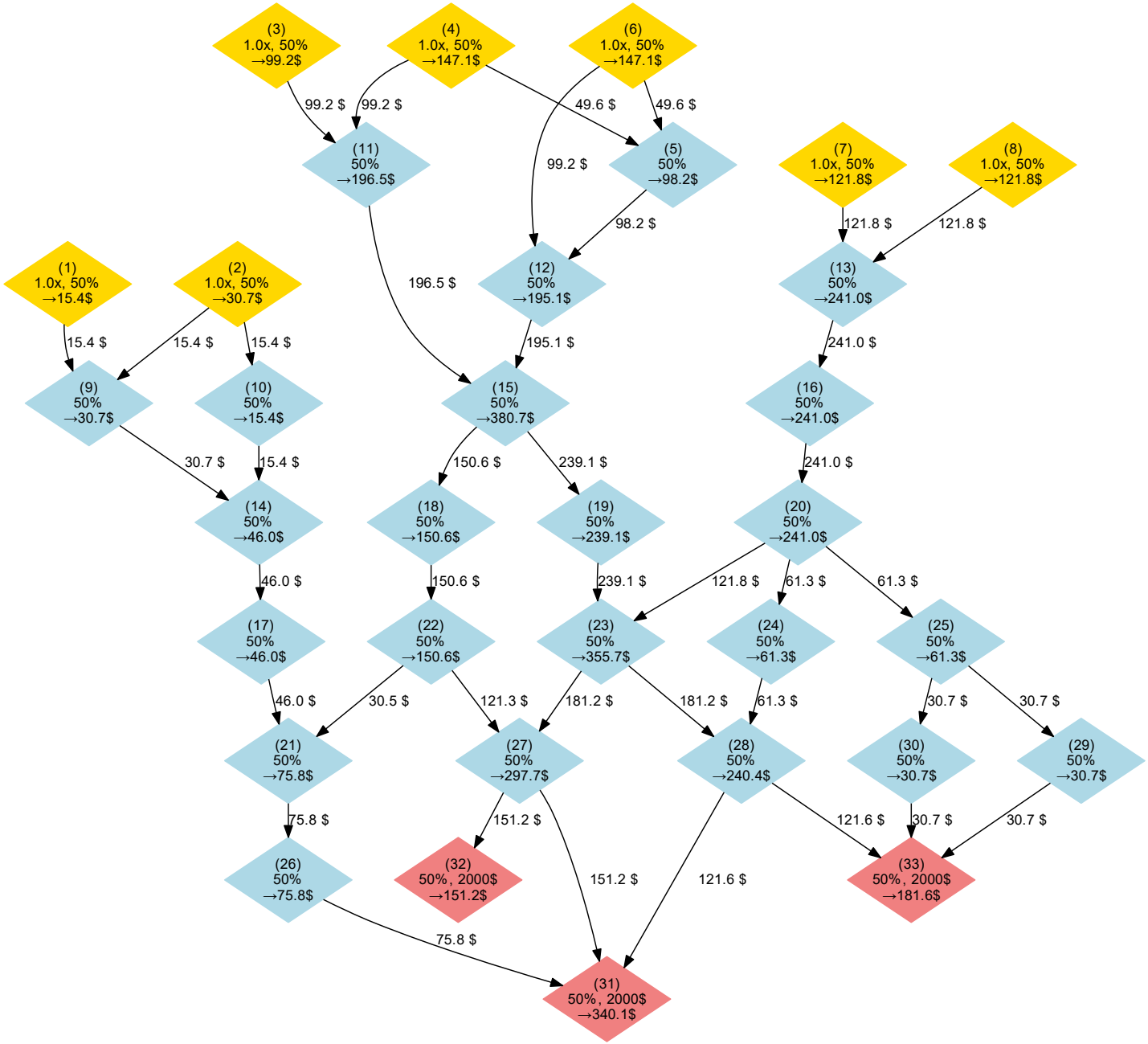
- Loss Exceedance Curve, Value at Risk

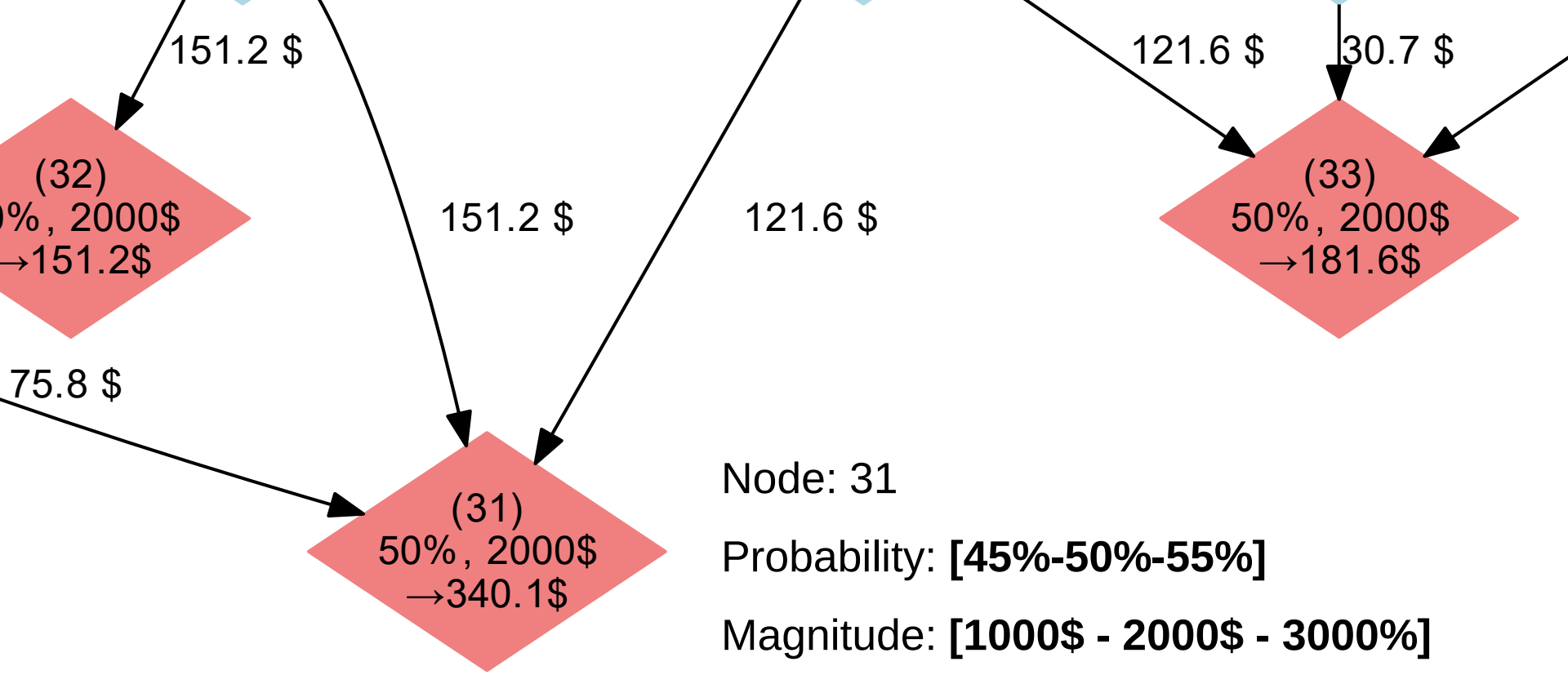
Loss Exceedance Curve





Examples & Applications


(3)
1.0x, 50%
→99.2$
(4)
1.0x, 50%
→147.1$
(6)
1.0x, 50%
→147.1$
99.2 $
99.2 $
49.6 $
49.6 $
(11)
50%
→196.5$
99.2 $
(5)
50%
→98.2$
(7)
1.0x, 50%
→121.8$
(8)
1.0x, 50%
→121.8$
98.2 $
121.8 $
121.8 $
(1)
1.0x, 50%
→15.4$
(2)
1.0x, 50%
→30.7$
196.5 $
(12)
50%
→195.1$
(13)
50%
→241.0$
15.4 $
15.4 $
15.4 $
195.1 $
241.0 $
(9)
50%
→30.7$
(10)
50%
→15.4$
(15)
50%
→380.7$
(16)
50%
→241.0$
30.7 $
15.4 $
150.6 $
239.1 $
241.0 $
(14)
50%
→46.0$
(18)
50%
→150.6$
(19)
50%
→239.1$
(20)
50%
→241.0$
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(17)
50%
→46.0$
(22)
50%
→150.6$
(23)
50%
→355.7$
(24)
50%
→61.3$
(25)
50%
→61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
(21)
50%
→75.8$
(27)
50%
→297.7$
(28)
50%
→240.4$
(30)
50%
→30.7$
(29)
50%
→30.7$
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
(26)
50%
→75.8$
(32)
50%, 2000$
→151.2$
151.2 $
121.6 $
(33)
50%, 2000$
→181.6$
75.8 $
(31)
50%, 2000$
→340.1$

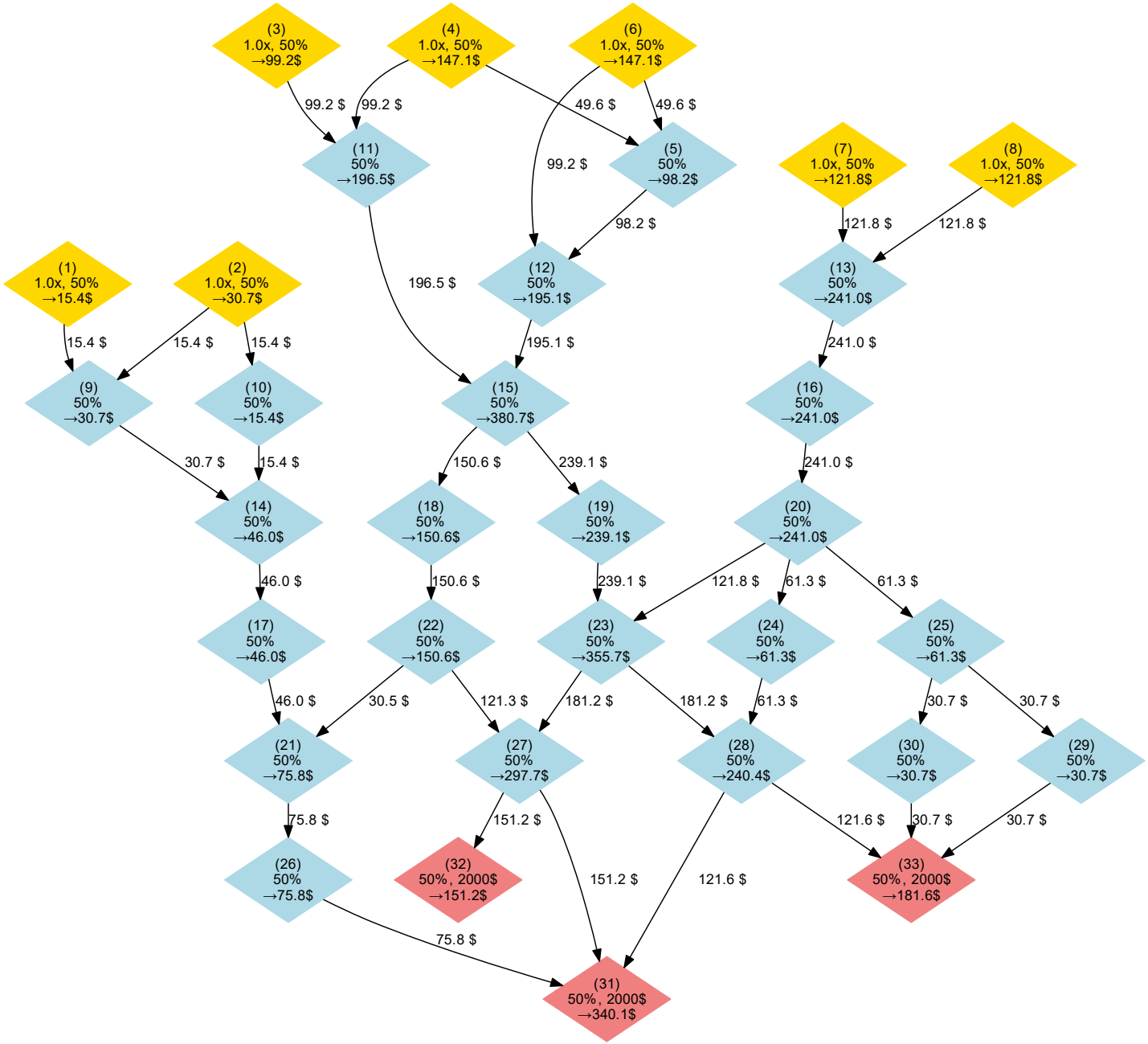


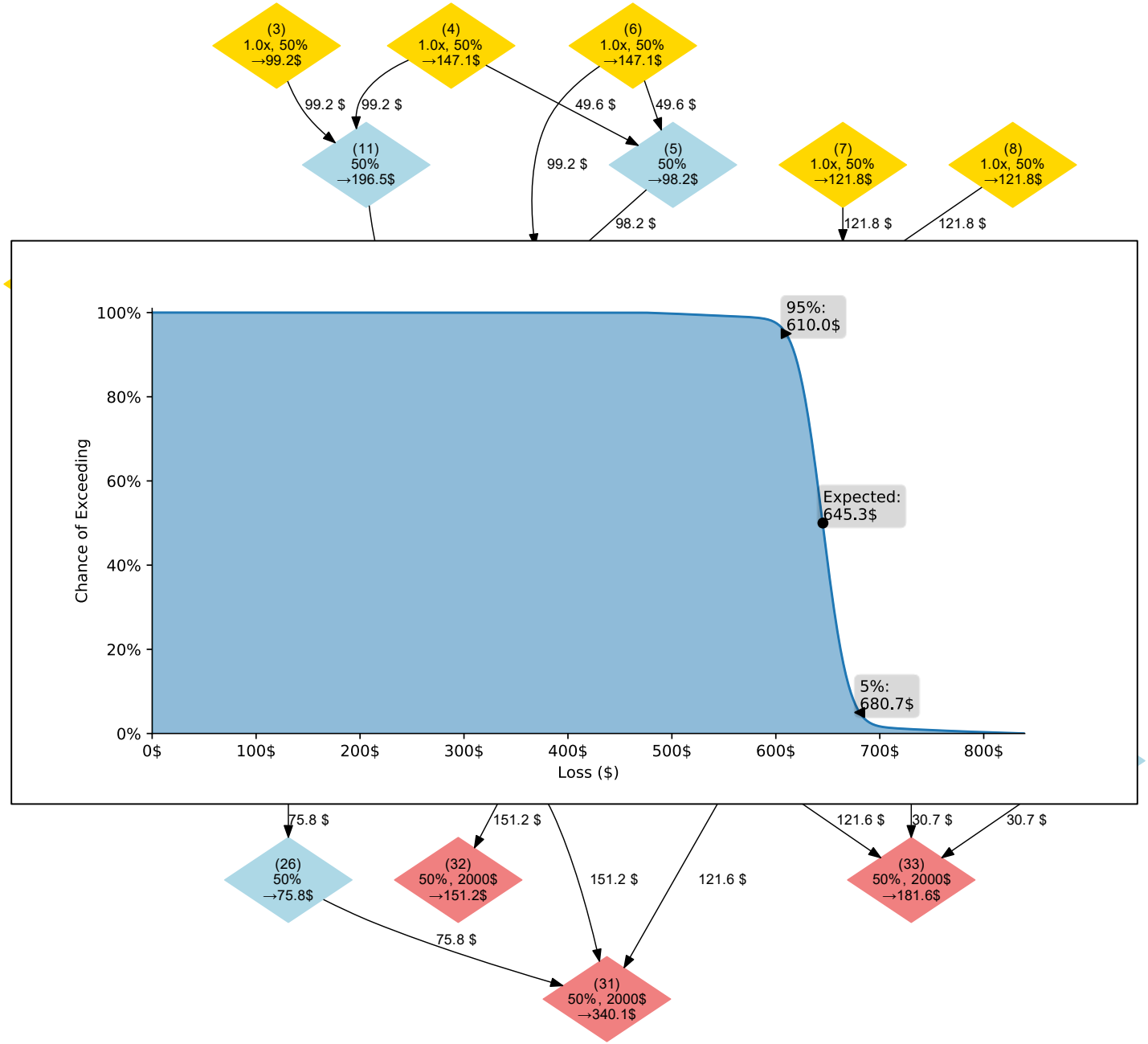
Node: 31

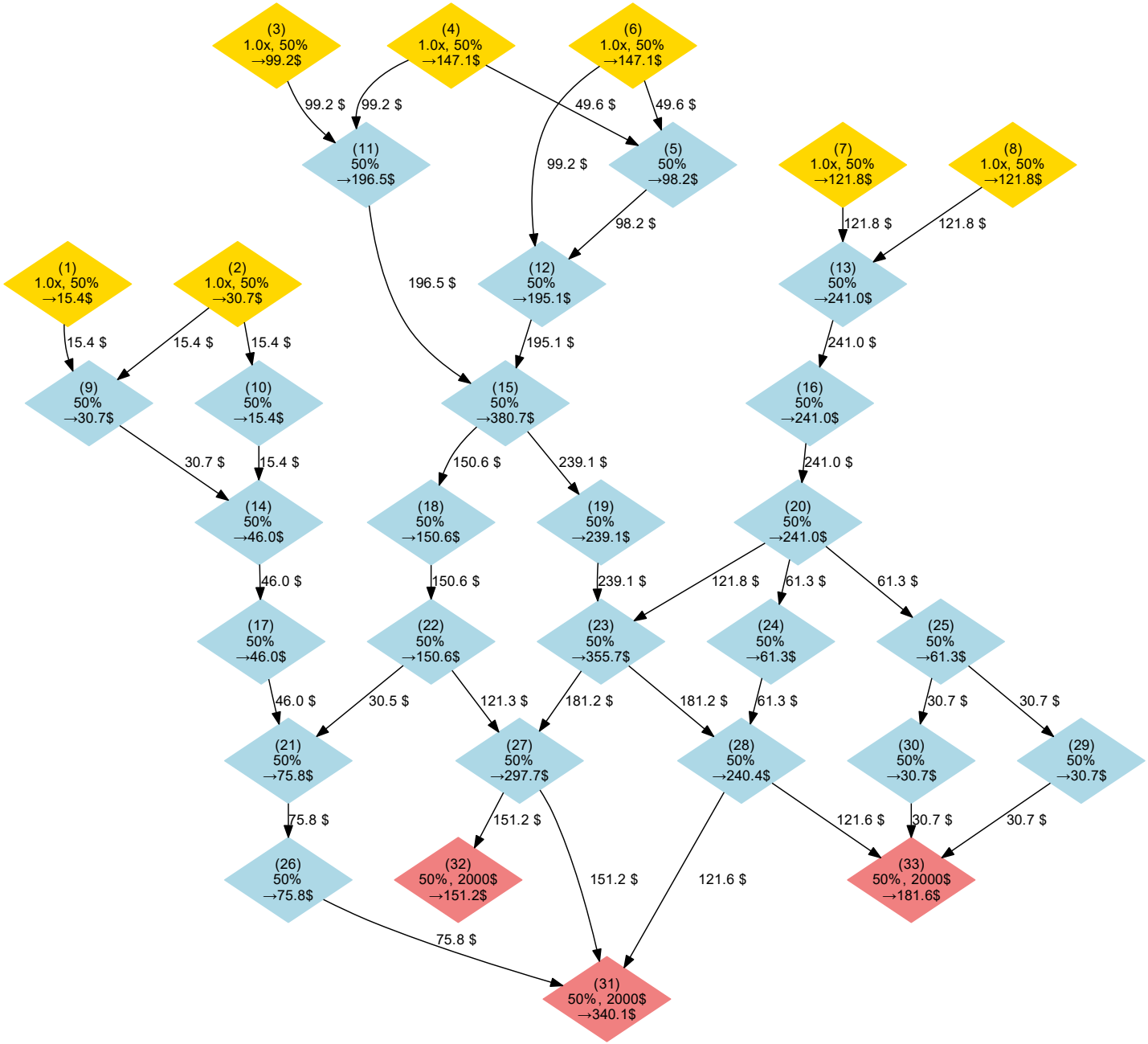
Probability: **[45%-50%-55%]**

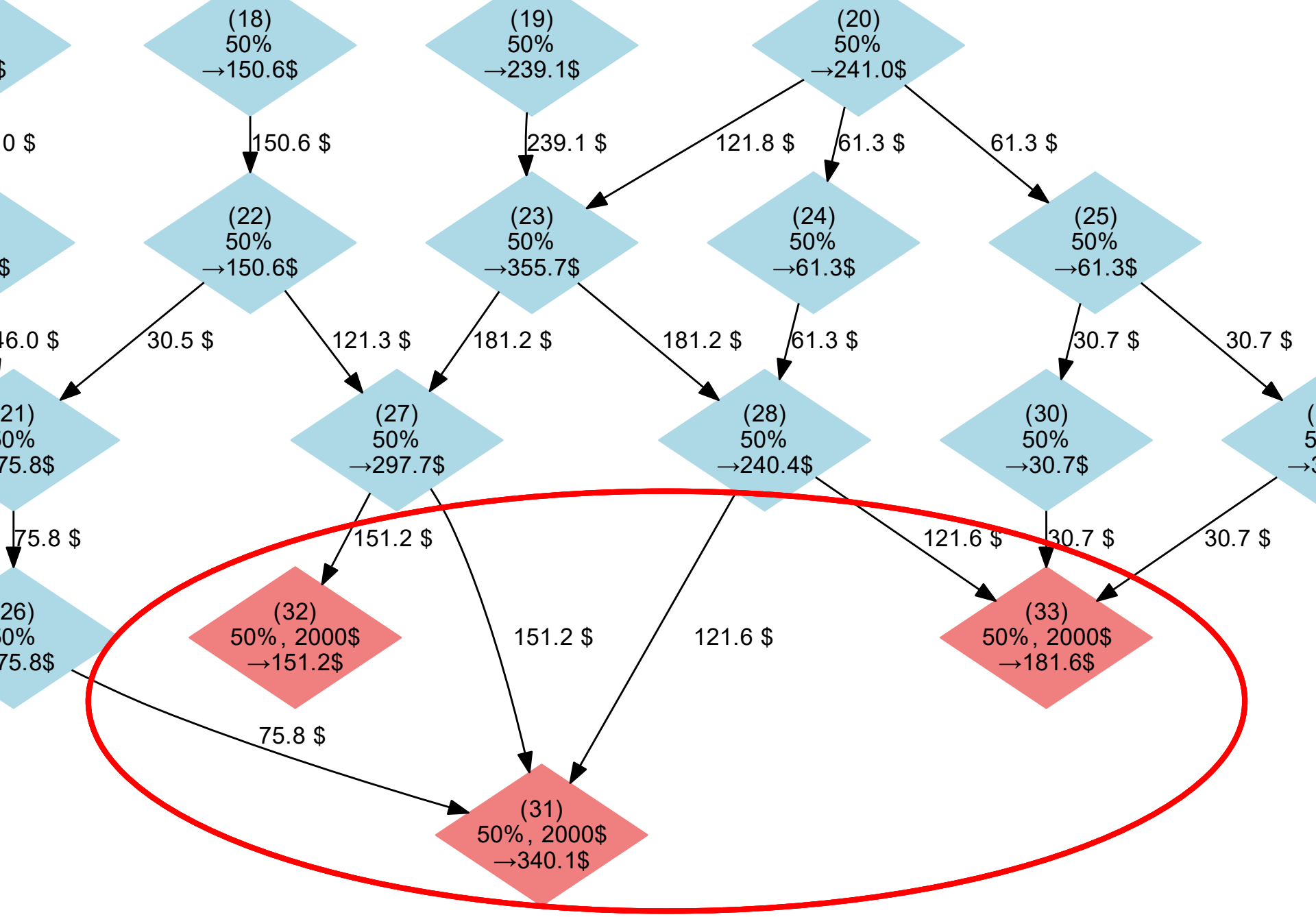
Magnitude: **[1000$ - 2000$ - 3000%]**

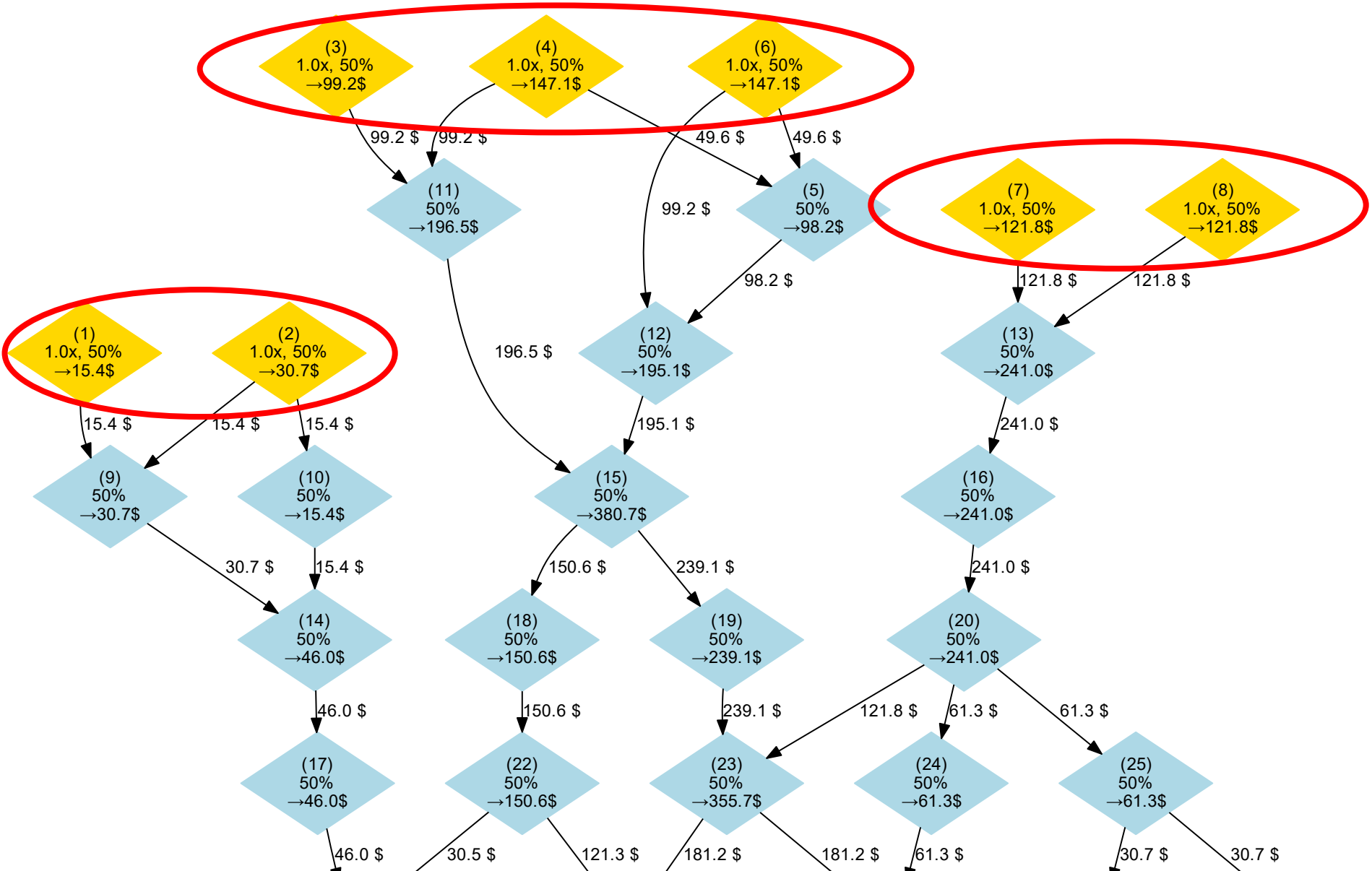
Resulting Risk: **340.1$**

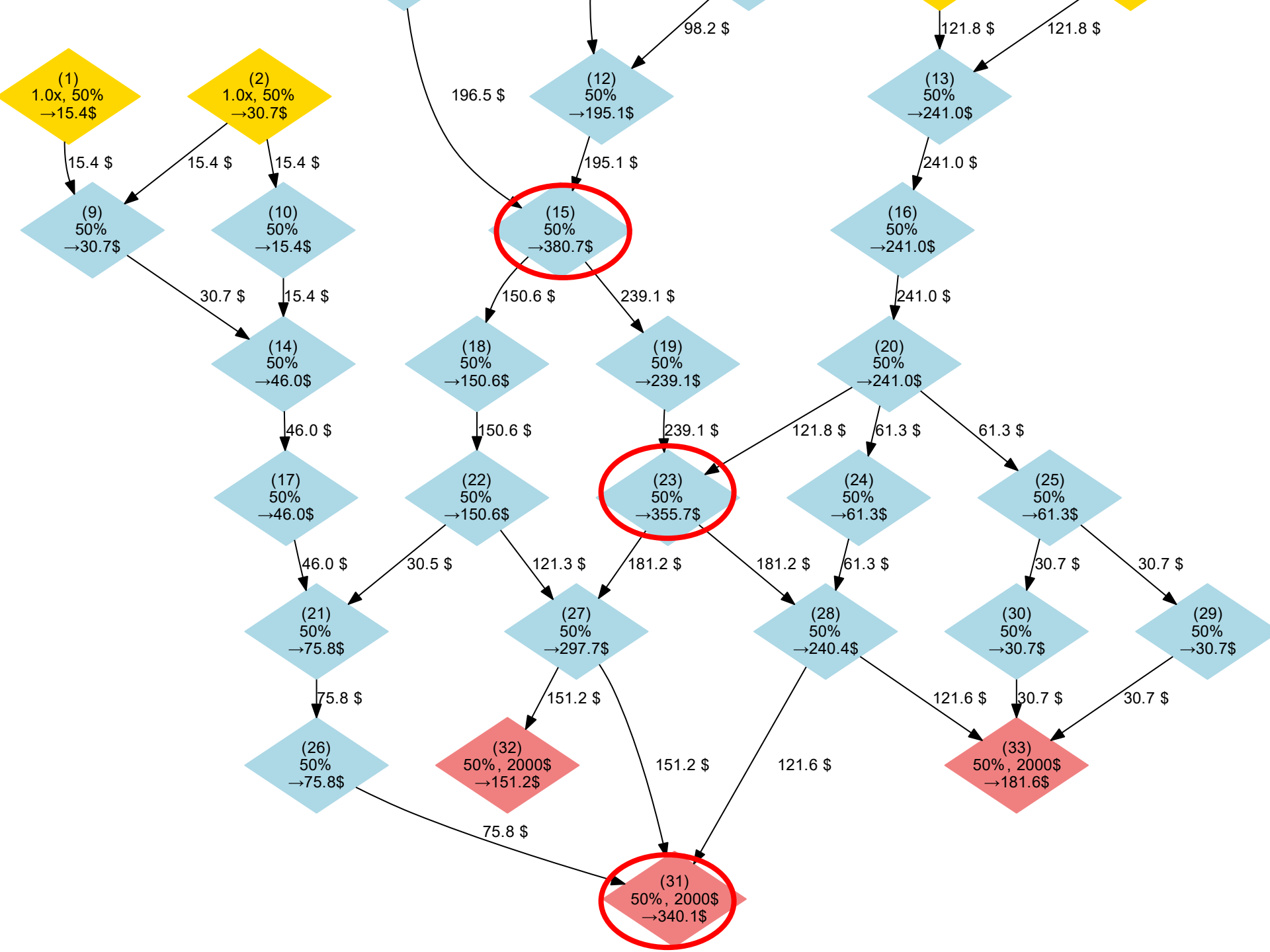

(3)
1.0x, 50%
→99.2$
(4)
1.0x, 50%
→147.1$
(6)
1.0x, 50%
→147.1$
99.2 $
99.2 $
49.6 $
49.6 $
(11)
50%
→196.5$
99.2 $
(5)
50%
→98.2$
(7)
1.0x, 50%
→121.8$
(8)
1.0x, 50%
→121.8$
98.2 $
121.8 $
121.8 $
(1)
1.0x, 50%
→15.4$
(2)
1.0x, 50%
→30.7$
196.5 $
(12)
50%
→195.1$
(13)
50%
→241.0$
15.4 $
15.4 $
15.4 $
195.1 $
241.0 $
(9)
50%
→30.7$
(10)
50%
→15.4$
(15)
50%
→380.7$
(16)
50%
→241.0$
30.7 $
15.4 $
150.6 $
239.1 $
241.0 $
(14)
50%
→46.0$
(18)
50%
→150.6$
(19)
50%
→239.1$
(20)
50%
→241.0$
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(17)
50%
→46.0$
(22)
50%
→150.6$
(23)
50%
→355.7$
(24)
50%
→61.3$
(25)
50%
→61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
(21)
50%
→75.8$
(27)
50%
→297.7$
(28)
50%
→240.4$
(30)
50%
→30.7$
(29)
50%
→30.7$
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
(26)
50%
→75.8$
(32)
50%, 2000$
→151.2$
151.2 $
121.6 $
(33)
50%, 2000$
→181.6$
75.8 $
(31)
50%, 2000$
→340.1$

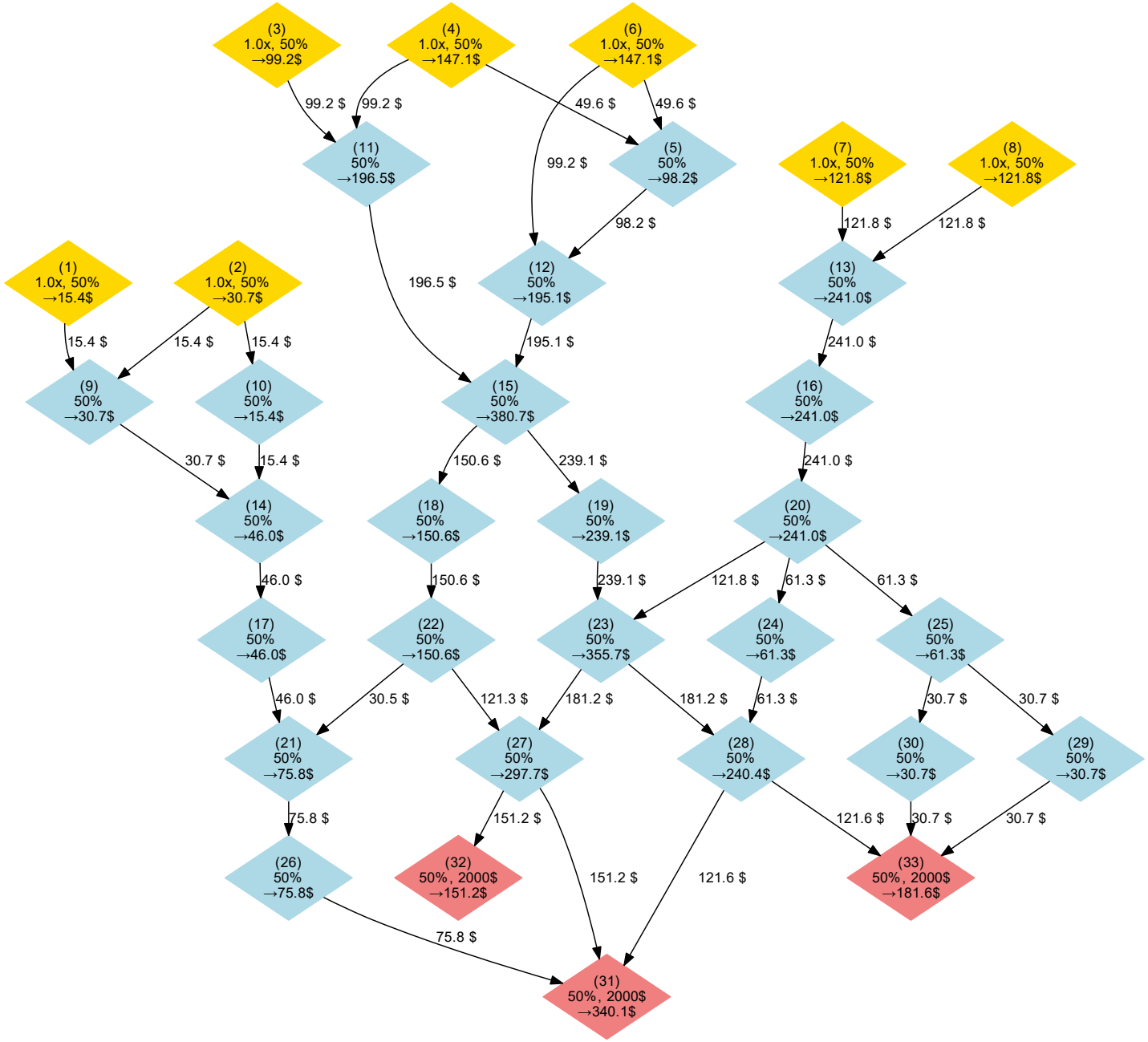

(3)
1.0x, 50%
→99.2$
(4)
1.0x, 50%
→147.1$
(6)
1.0x, 50%
→147.1$
99.2 $
99.2 $
49.6 $
49.6 $
(11)
50%
→196.5$
99.2 $
(5)
50%
→98.2$
(7)
1.0x, 50%
→121.8$
(8)
1.0x, 50%
→121.8$
98.2 $
121.8 $
121.8 $
100%
80%
60%
40%
20%
0%
Chance of Exceeding
95%:
610.0$
Expected:
645.3$
5%:
680.7$
0$
100$
200$
300$
400$
500$
600$
700$
800$
Loss ($)
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
(26)
50%
→75.8$
(32)
50%, 2000$
→151.2$
151.2 $
121.6 $
(33)
50%, 2000$
→181.6$
75.8 $
(31)
50%, 2000$
→340.1$

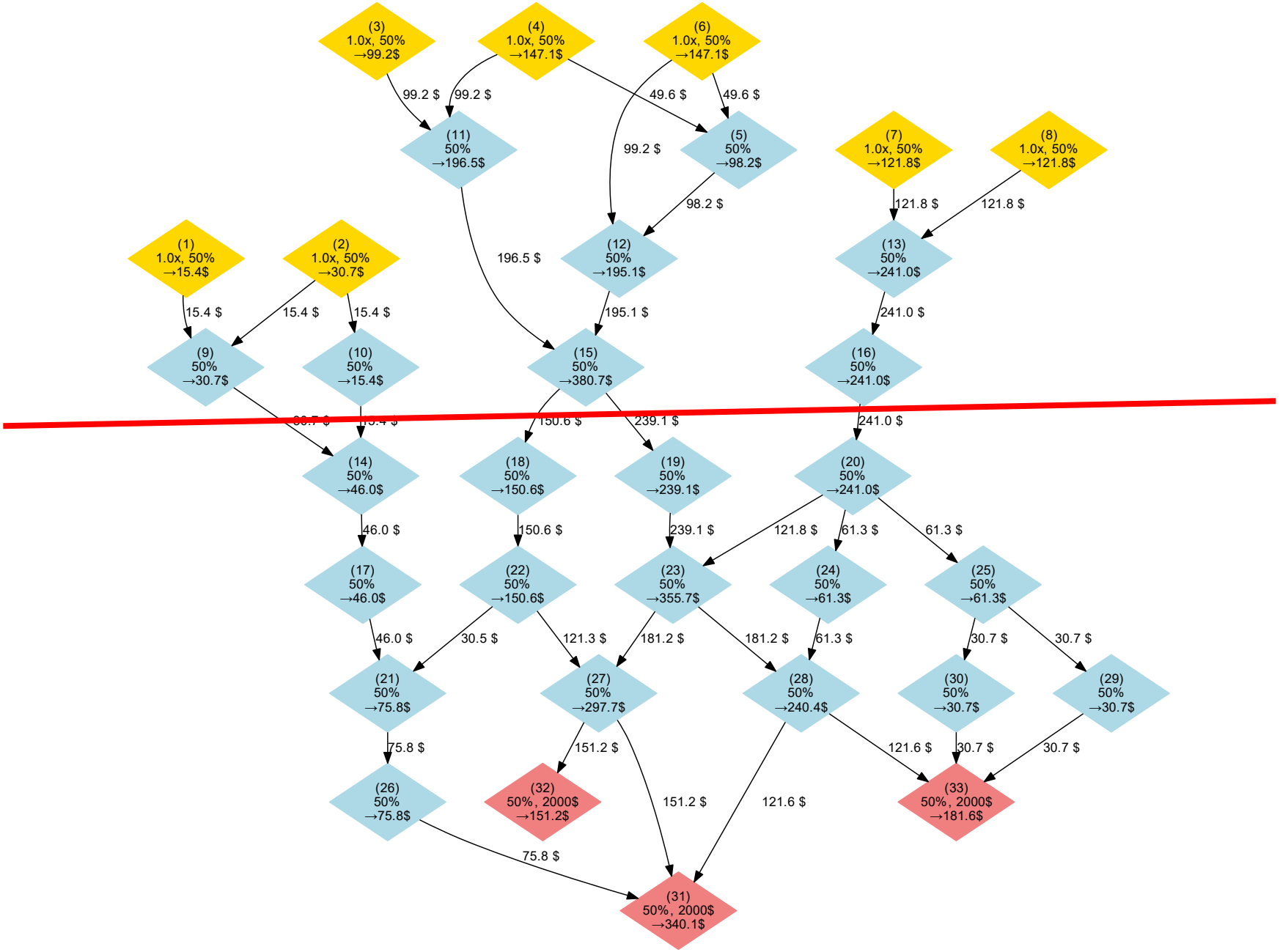

(3)
1.0x, 50%
→99.2$
(4)
1.0x, 50%
→147.1$
(6)
1.0x, 50%
→147.1$
99.2 $
99.2 $
49.6 $
49.6 $
(11)
50%
→196.5$
99.2 $
(5)
50%
→98.2$
(7)
1.0x, 50%
→121.8$
(8)
1.0x, 50%
→121.8$
98.2 $
121.8 $
121.8 $
(1)
1.0x, 50%
→15.4$
(2)
1.0x, 50%
→30.7$
196.5 $
(12)
50%
→195.1$
(13)
50%
→241.0$
15.4 $
15.4 $
15.4 $
195.1 $
241.0 $
(9)
50%
→30.7$
(10)
50%
→15.4$
(15)
50%
→380.7$
(16)
50%
→241.0$
30.7 $
15.4 $
150.6 $
239.1 $
241.0 $
(14)
50%
→46.0$
(18)
50%
→150.6$
(19)
50%
→239.1$
(20)
50%
→241.0$
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(17)
50%
→46.0$
(22)
50%
→150.6$
(23)
50%
→355.7$
(24)
50%
→61.3$
(25)
50%
→61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
(21)
50%
→75.8$
(27)
50%
→297.7$
(28)
50%
→240.4$
(30)
50%
→30.7$
(29)
50%
→30.7$
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
(26)
50%
→75.8$
(32)
50%, 2000$
→151.2$
151.2 $
121.6 $
(33)
50%, 2000$
→181.6$
75.8 $
(31)
50%, 2000$
→340.1$

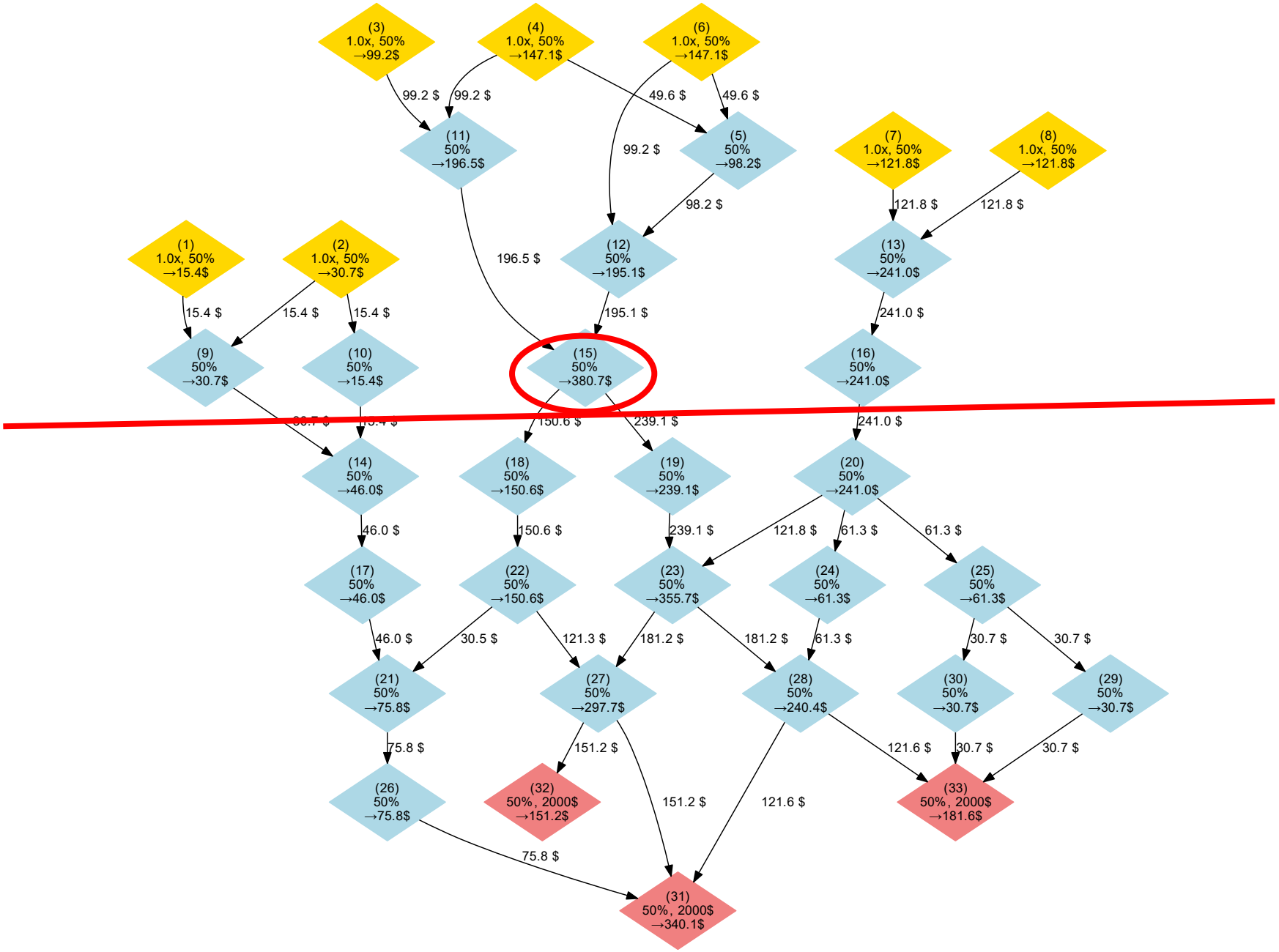

(18)
50%
→150.6$
(19)
50%
→239.1$
(20)
50%
→241.0$
0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(22)
50%
→150.6$
(23)
50%
→355.7$
(24)
50%
→61.3$
(25)
50%
→61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
21)
0%
75.8$
(27)
50%
→297.7$
(28)
50%
→240.4$
(30)
50%
→30.7$
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
26)
0%
75.8$
(32)
50%, 2000$
→151.2$
151.2 $
121.6 $
(33)
50%, 2000$
→181.6$
75.8 $
(31)
50%, 2000$
→340.1$

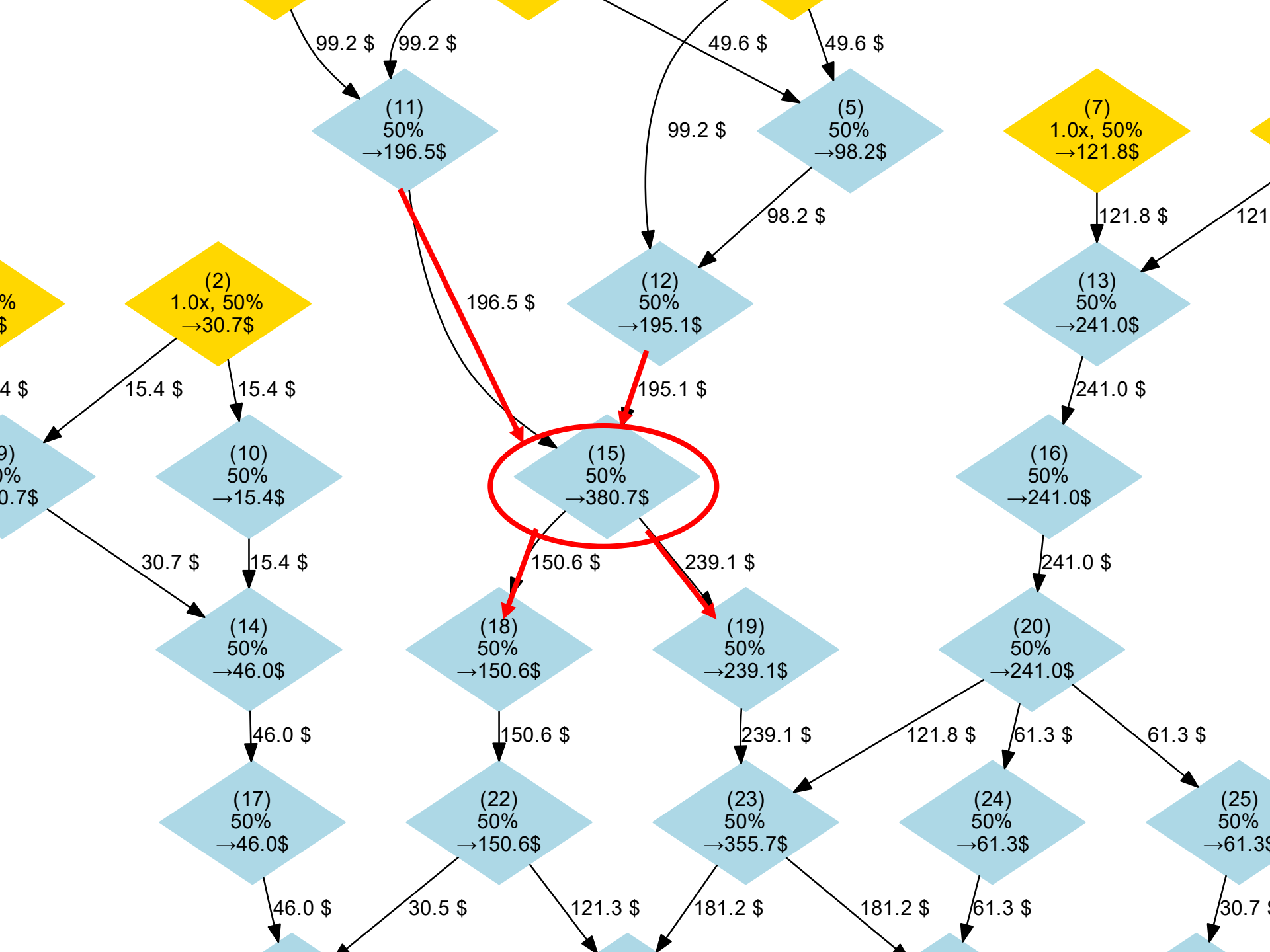

(3)
1.0x, 50%
→99.2$
(4)
1.0x, 50%
→147.1$
(6)
1.0x, 50%
→147.1$
99.2 $
99.2 $
49.6 $
49.6 $
(11)
50%
→196.5$
99.2 $
(5)
50%
→98.2$
(7)
1.0x, 50%
→121.8$
(8)
1.0x, 50%
→121.8$
98.2 $
121.8 $
121.8 $
(1)
1.0x, 50%
→15.4$
(2)
1.0x, 50%
→30.7$
196.5 $
(12)
50%
→195.1$
(13)
50%
→241.0$
15.4 $
15.4 $
15.4 $
195.1 $
241.0 $
(9)
50%
→30.7$
(10)
50%
→15.4$
(15)
50%
→380.7$
(16)
50%
→241.0$
30.7 $
15.4 $
150.6 $
239.1 $
241.0 $
(14)
50%
→46.0$
(18)
50%
→150.6$
(19)
50%
→239.1$
(20)
50%
→241.0$
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(17)
50%
→46.0$
(22)
50%
→150.6$
(23)
50%
→355.7$
(24)
50%
→61.3$
(25)
50%
→61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $

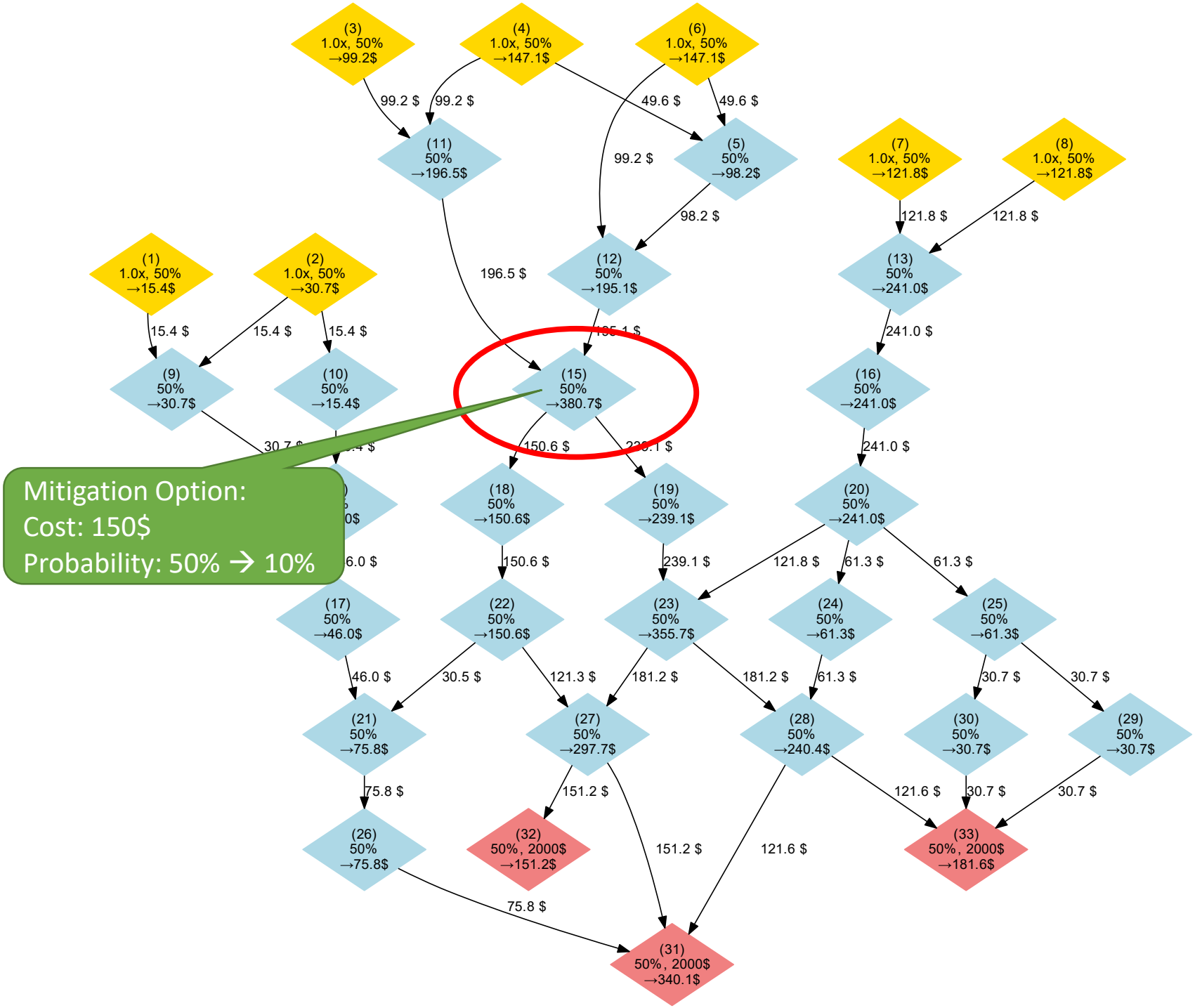

(1)
1.0x, 50%
→15.4$
(2)
1.0x, 50%
→30.7$
(9)
50%
→30.7$
(10)
50%
→15.4$
(12)
50%
→195.1$
(13)
50%
→241.0$
(14)
50%
→46.0$
(15)
50%
→380.7$
(16)
50%
→241.0$
(17)
50%
→46.0$
(18)
50%
→150.6$
(19)
50%
→239.1$
(20)
50%
→241.0$
(21)
50%
→75.8$
(22)
50%
→150.6$
(23)
50%
→355.7$
(24)
50%
→61.3$
(25)
50%
→61.3$
(26)
50%
→75.8$
(27)
50%
→297.7$
(28)
50%
→240.4$
(29)
50%
→30.7$
(30)
50%
→30.7$
(31)
50%, 2000$
→340.1$
(32)
50%, 2000$
→151.2$
(33)
50%, 2000$
→181.6$
15.4 $
15.4 $
15.4 $
196.5 $
98.2 $
121.8 $
121.8 $
195.1 $
241.0 $
30.7 $
15.4 $
150.6 $
239.1 $
241.0 $
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
151.2 $
121.6 $
75.8 $

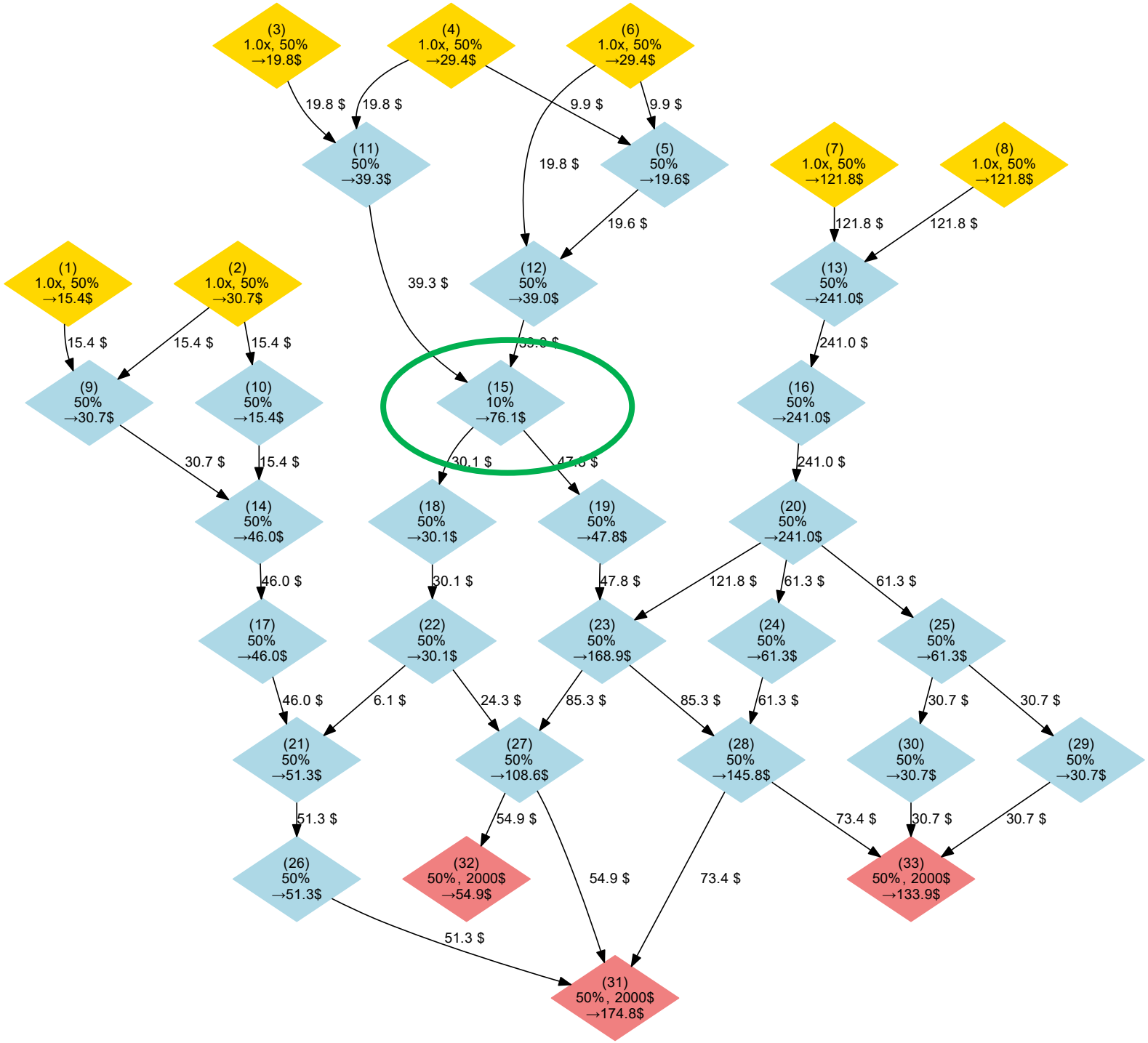

(3)
1.0x, 50%
→99.2$
(4)
1.0x, 50%
→147.1$
(6)
1.0x, 50%
→147.1$
99.2 $
99.2 $
49.6 $
49.6 $
(11)
50%
→196.5$
99.2 $
(5)
50%
→98.2$
(7)
1.0x, 50%
→121.8$
(8)
1.0x, 50%
→121.8$
98.2 $
121.8 $
121.8 $
(1)
1.0x, 50%
→15.4$
(2)
1.0x, 50%
→30.7$
196.5 $
(12)
50%
→195.1$
(13)
50%
→241.0$
15.4 $
15.4 $
15.4 $
195.1 $
241.0 $
(9)
50%
→30.7$
(10)
50%
→15.4$
(15)
50%
→380.7$
(16)
50%
→241.0$
30.7 $
15.4 $
150.6 $
239.1 $
241.0 $
(14)
50%
→46.0$
(18)
50%
→150.6$
(19)
50%
→239.1$
(20)
50%
→241.0$
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(17)
50%
→46.0$
(22)
50%
→150.6$
(23)
50%
→355.7$
(24)
50%
→61.3$
(25)
50%
→61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
(21)
50%
→75.8$
(27)
50%
→297.7$
(28)
50%
→240.4$
(30)
50%
→30.7$
(29)
50%
→30.7$
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
(26)
50%
→75.8$
(32)
50%, 2000$
→151.2$
151.2 $
121.6 $
(33)
50%, 2000$
→181.6$
75.8 $
(31)
50%, 2000$
→340.1$

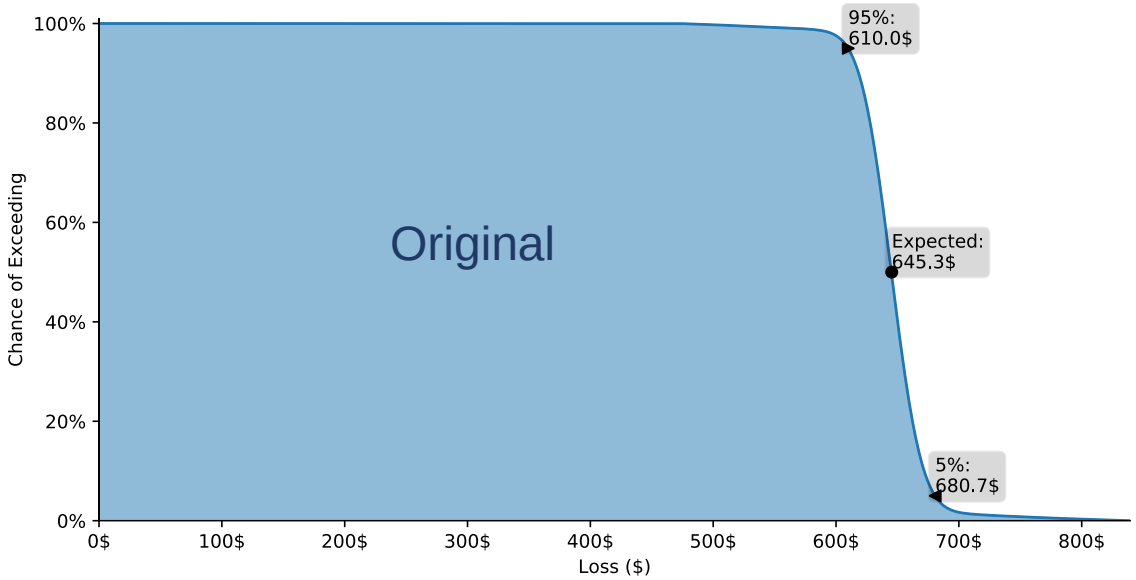

(3) 1.0x, 50% →99.2$
(4) 1.0x, 50% →147.1$
(6) 1.0x, 50% →147.1$
99.2 $
99.2 $
49.6 $
49.6 $
(11) 50% →196.5$
99.2 $
(5) 50% →98.2$
(7) 1.0x, 50% →121.8$
(8) 1.0x, 50% →121.8$
98.2 $
121.8 $
121.8 $
(1) 1.0x, 50% →15.4$
(2) 1.0x, 50% →30.7$
196.5 $
(12) 50% →195.1$
(13) 50% →241.0$
15.4 $
15.4 $
15.4 $
195.1 $
241.0 $
(9) 50% →30.7$
(10) 50% →15.4$
(15) 50% →380.7$
(16) 50% →241.0$
150.6 $
239.1 $
241.0 $
(14) 50% →46.0$
(18) 50% →150.6$
(19) 50% →239.1$
(20) 50% →241.0$
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(17) 50% →46.0$
(22) 50% →150.6$
(23) 50% →355.7$
(24) 50% →61.3$
(25) 50% →61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
(21) 50% →75.8$
(27) 50% →297.7$
(28) 50% →240.4$
(30) 50% →30.7$
(29) 50% →30.7$
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
(26) 50% →75.8$
(32) 50%, 2000$ →151.2$
151.2 $
121.6 $
(33) 50%, 2000$ →181.6$
75.8 $
(31) 50%, 2000$ →340.1$

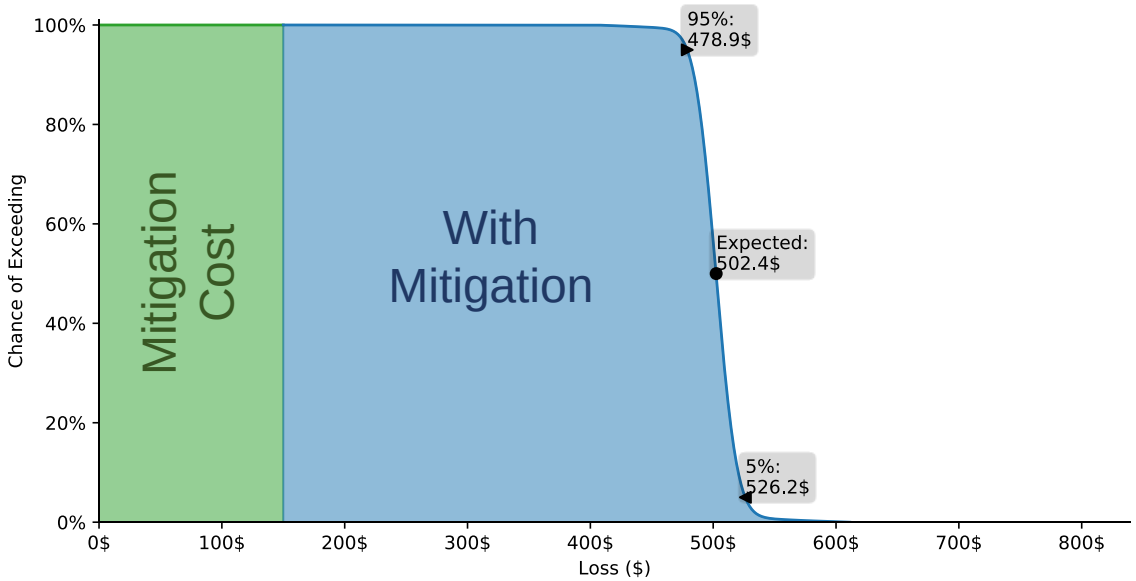

(3) 1.0x, 50% →99.2$
(4) 1.0x, 50% →147.1$
(6) 1.0x, 50% →147.1$
99.2 $
99.2 $
49.6 $
49.6 $
(11) 50% →196.5$
99.2 $
(5) 50% →98.2$
(7) 1.0x, 50% →121.8$
(8) 1.0x, 50% →121.8$
98.2 $
121.8 $
121.8 $
(1) 1.0x, 50% →15.4$
(2) 1.0x, 50% →30.7$
196.5 $
(12) 50% →195.1$
(13) 50% →241.0$
15.4 $
15.4 $
15.4 $
195.1 $
241.0 $
(9) 50% →30.7$
(10) 50% →15.4$
(15) 50% →380.7$
(16) 50% →241.0$
150.6 $
239.1 $
241.0 $
(14) 50% →46.0$
(18) 50% →150.6$
(19) 50% →239.1$
(20) 50% →241.0$
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(17) 50% →46.0$
(22) 50% →150.6$
(23) 50% →355.7$
(24) 50% →61.3$
(25) 50% →61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
(21) 50% →75.8$
(27) 50% →297.7$
(28) 50% →240.4$
(30) 50% →30.7$
(29) 50% →30.7$
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
(26) 50% →75.8$
(32) 50%, 2000$ →151.2$
151.2 $
121.6 $
(33) 50%, 2000$ →181.6$
75.8 $
(31) 50%, 2000$ →340.1$


99.2 $
99.2 $
49.6 $
49.6 $
(11)
50%
→196.5$
99.2 $
(5)
50%
→98.2$
(7)
1.0x, 50%
→121.8$
98.2 $
121.8 $
(2)
1.0x, 50%
→30.7$
196.5 $
(12)
50%
→195.1$
(13)
50%
→241.0$
15.4 $
15.4 $
195.1 $
241.0 $
(10)
50%
→15.4$
(15)
50%
→380.7$
(16)
50%
→241.0$
30.7 $
15.4 $
150.6 $
239.1 $
241.0 $
(14)
50%
→46.0$
(18)
50%
→150.6$
(19)
50%
→239.1$
(20)
50%
→241.0$
46.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
(17)
50%
→46.0$
(22)
50%
→150.6$
(23)
50%
→355.7$
(24)
50%
→61.3$
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $


(3) 1.0x, 50% →99.2$
(4) 1.0x, 50% →147.1$
(6) 1.0x, 50% →147.1$
(7) 1.0x, 50% →121.8$
(8) 1.0x, 50% →121.8$
(1) 1.0x, 50% →15.4$
(2) 1.0x, 50% →30.7$
(11) 50% →196.5$
(5) 50% →98.2$
(12) 50% →195.1$
(13) 50% →241.0$
(9) 50% →30.7$
(10) 50% →15.4$
(15) 50% →380.7$
(16) 50% →241.0$
(18) 50% →150.6$
(19) 50% →239.1$
(20) 50% →241.0$
(17) 50% →46.0$
(22) 50% →150.6$
(23) 50% →355.7$
(24) 50% →61.3$
(25) 50% →61.3$
(21) 50% →75.8$
(27) 50% →297.7$
(28) 50% →240.4$
(30) 50% →30.7$
(29) 50% →30.7$
(26) 50% →75.8$
(32) 50%, 2000$ →151.2$
(33) 50%, 2000$ →181.6$
(31) 50%, 2000$ →340.1$
99.2 $
99.2 $
49.6 $
49.6 $
99.2 $
98.2 $
121.8 $
121.8 $
196.5 $
15.4 $
15.4 $
15.4 $
241.0 $
150.6 $
241.0 $
150.6 $
239.1 $
121.8 $
61.3 $
61.3 $
46.0 $
30.5 $
121.3 $
181.2 $
181.2 $
61.3 $
30.7 $
30.7 $
75.8 $
151.2 $
121.6 $
30.7 $
30.7 $
151.2 $
121.6 $
75.8 $
Mitigation Option:
Cost: 150$
Probability: 50% → 10%

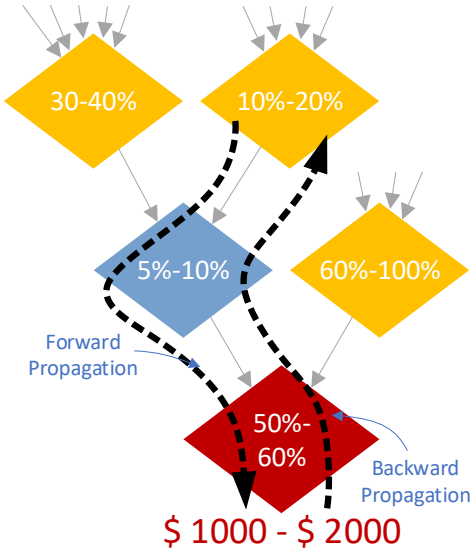

(3) 1.0x, 50% →19.8$
(4) 1.0x, 50% →29.4$
(6) 1.0x, 50% →29.4$
19.8 $
19.8 $
9.9 $
9.9 $
(11) 50% →39.3$
19.8 $
(5) 50% →19.6$
(7) 1.0x, 50% →121.8$
(8) 1.0x, 50% →121.8$
19.6 $
121.8 $
121.8 $
(1) 1.0x, 50% →15.4$
(2) 1.0x, 50% →30.7$
39.3 $
(12) 50% →39.0$
(13) 50% →241.0$
15.4 $
15.4 $
15.4 $
241.0 $
(9) 50% →30.7$
(10) 50% →15.4$
(15) 10% →76.1$
(16) 50% →241.0$
30.7 $
15.4 $
30.1 $
241.0 $
(14) 50% →46.0$
(18) 50% →30.1$
(19) 50% →47.8$
(20) 50% →241.0$
46.0 $
30.1 $
47.8 $
121.8 $
61.3 $
61.3 $
(17) 50% →46.0$
(22) 50% →30.1$
(23) 50% →168.9$
(24) 50% →61.3$
(25) 50% →61.3$
46.0 $
6.1 $
24.3 $
85.3 $
85.3 $
61.3 $
30.7 $
30.7 $
(21) 50% →51.3$
(27) 50% →108.6$
(28) 50% →145.8$
(30) 50% →30.7$
(29) 50% →30.7$
51.3 $
54.9 $
73.4 $
30.7 $
30.7 $
(26) 50% →51.3$
(32) 50%, 2000$ →54.9$
54.9 $
73.4 $
(33) 50%, 2000$ →133.9$
51.3 $
(31) 50%, 2000$ →174.8$

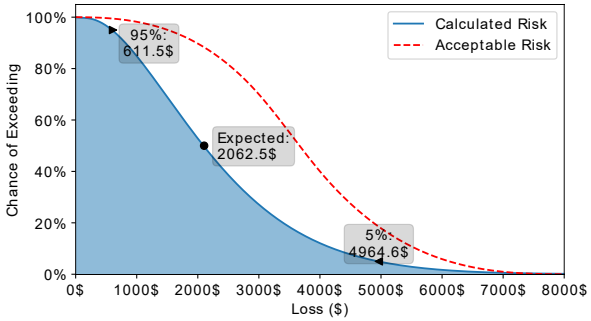

Original
95%:
610.0$
Expected:
645.3$
5%:
680.7$
Chance of Exceeding
100%
80%
60%
40%
20%
0%
0$
100$
200$
300$
400$
500$
600$
700$
800$
Loss ($)


Mitigation Cost
With Mitigation
95%:
478.9$
Expected:
502.4$
5%:
526.2$
Chance of Exceeding
100%
80%
60%
40%
20%
0%
0$
100$
200$
300$
400$
500$
600$
700$
800$
Loss ($)

Conclusion / Take-Aways

- RISKEE is a method for quantitatively assessing risks as probability distributions (incl. uncertainty!)
- Risk-Trees: attack trees with risk attributes (frequency, probability, impact)
- Result:
  - Loss Exceedance Curve
  - Risk Contribution for each node
  - Graph Analysis of Risk-Tree





WEIL WIR'S GENIESSEN
SERFAUS-FISS-LADIS

Bagjump in
Serfaus/Fiss/Ladis
Tyrol, Austria