TACTICAL TARA - SAFETY-CRITICAL OR CHECKBOX COMPLIANCE

URBAN JONSON

SVP IT AND CYBERSECURITY SERVICES

SERJON, LLC

URBAN JONSON

ujonson@serjon.com

Current

- SVP Information Technology and Cybersecurity Services, SERJON, LLC
- US FBI InfraGard Transportation Subject Matter Expert
- FBI Automotive Sector Specific Working Group (SSWG)
- Board of Directors, Cyber Truck Challenge
- Program Committee, ESCAR USA
- SAE Vehicle Electrical System Security Committee Member
- Technology & Maintenance Council (TMC) S.5 and S.12 Study Group Member

Experience

- Over 35 years of experience in IT and Cybersecurity, including strategic planning, assessments, project management, and program management
- Various papers, talks, and research on hacking, as well as defending trucks and transportation in general
- Abusing and defending systems since the 1980s

AGENDA

- Why this topic?
- Threat Analysis and Risk Assessment (TARA) Overview
- Organizational Structure
- Supply Chain Observations
- Common Issues
- Conclusions
- How to Improve
- Process Improvement
- 30,000 ft View
- Industry Developments

WHY THIS TOPIC?

OH LOOK…SQUIRREL!

- Working for over 40 years in technology in various environments
- Benefit of insight by just looking at the situation
- Experience leads to process improvement insights
- A discussion with a prospective client prompted ***The Quest***
  - Reported an overwhelming stack of TARA documents and other security artifacts, such as pen testing reports, in need of review, mainly in Word and XLS
  - Issues with quality and consistency
  - Rework and corrections were required
  - All the hallmark indicators of broken business processes

THE QUEST

- Interview industry stakeholders about their use of TARAs
  - OEMs
  - Tier1 Suppliers
  - TARA Tool Providers
  - Industry Experts
  - Regulatory Authorities
- Look at tactical execution versus the theory
- Determine if TARAs are treated as a living critical safety artifact or just a check box compliance nuisance for type approval, or something in between

THE RULES

- Cast a wide net and interview as many organizations as possible
- All input into the study was “off the record”
- No attributions can be made to any organization
- Share what is beneficial to industry, no whining or soap box lectures
- Share general ideas that all organizations can use to improve TARA products and processes

TARA OVERVIEW

WHAT IS A TARA?

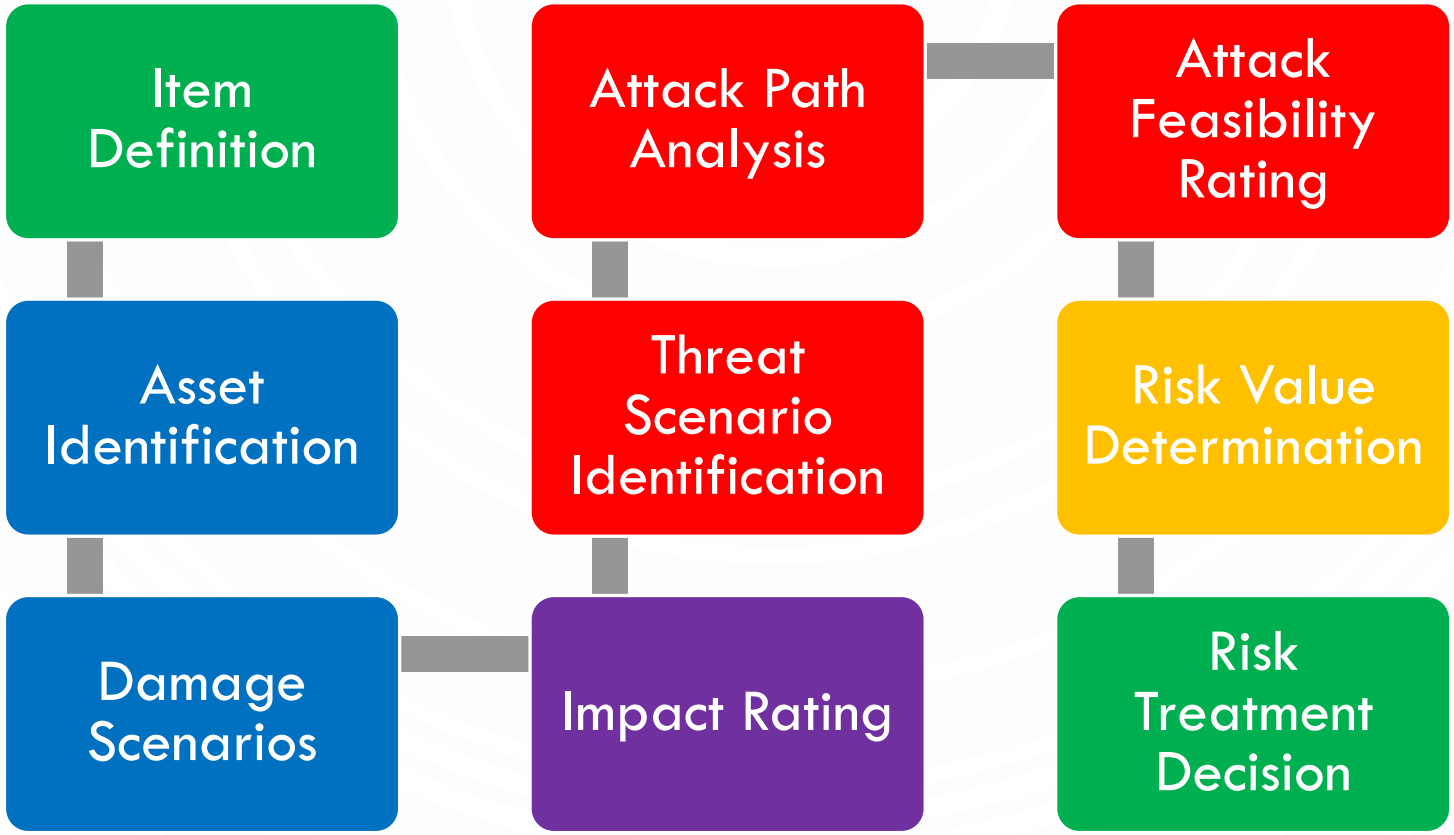
WHAT IS A TARA?

- Threat Analysis and Risk Assessment (TARA)
- Initially conducted during the design phase of product development
- Conducted from the attacker's point of view, which requires an understanding of adversaries, different attack paths, and the feasibility of attacks
- Commonly used within the ISO/SAE 21434 standard

WHAT IS A TARA?

- It is unlike penetration testing, which is focused on a completed product but can incorporate results of a pen test
- Similar to architectural risk analysis
- Specific steps vary depending on the approach and models used
- Can help identify critical areas and components for 3rd party PEN testing

ISO/SAE 21434 TARA PROCESS



TARA STEPS (ISO/SAE 21424)

- **Item Definition**
  - Boundaries, functions, preliminary architecture
- **Asset Identification**
  - Data and functional assets, cybersecurity properties (CIA), damage scenarios
- **Impact Rating**
  - Rates the impact of the damage scenarios (Major, Severe, etc.)
  - ISO/SAE 21434 Annex F – *Guidelines for impact rating*
- **Threat Scenario Identification**
  - STRIDE, Attack Trees, PASTA, DREAD, Known Vulnerabilities (CVEs)
  - UNECE R155 Annex 5 – *List of threats and corresponding mitigations*

TARA STEPS (ISO/SAE 21424)

- **Attack Path Analysis**
  - Routes or paths for exploitation
  - Require an attacker's mindset
- **Attack Feasibility Rating**
  - Required knowledge, resources, time, and effort
  - ISO/SAE 21434 Annex G – *Guidelines for attack feasibility rating*
- **Risk Value Determination**
  - Combination of risk impact and feasibility
- **Risk Treatment Decision**
  - Reducing, mitigating, or accepting the risk

ALTERNATE TARA PROCESS

TARA STEPS (ALT)

- **Asset Identification**
  - Communication interfaces, software modules, sensors, actuators, data, etc.
- **System Characterization**
  - External/internal interfaces, dependencies, interactions, data flows (including data flow diagrams, architecture diagrams
- **Threat Scenario Identification**
  - STRIDE, PASTA, DREAD, Attack Trees
  - UNECE R155 Annex 5 – *List of threats and corresponding mitigations*, GB 44495 and 44496, Auto-ISAC Threat Matrix, known vulnerabilities (CVEs)
- **Attack Feasibility Ratings**
  - Required knowledge, resources, time, and effort
  - ISO/SAE 21434 Annex G - *Guidelines for attack feasibility rating*

TARA STEPS (ALT)

- **Impact Rating**
  - Rates the impact of the damage scenarios (Major, Severe, etc.)
  - ISO/SAE 21434 Annex F– *Guidelines for impact rating*
- **Risk Determination**
  - Combination of risk impact and feasibility (use risk matrix or R=I X AF)
- **Risk Treatment Decisions**
  - Mitigate, Avoid, Transfer, Accept
- **Documentation and Traceability**
  - Record assumptions, assessments, and decisions
  - Ensure traceability between assets, threats, and controls
- **Review and Update**
  - Revisit TARA when item is updated or design changes
  - Update based on pen-testing, fuzzing, or new vulnerabilities

PROCESS TAKE AWAY

- TARA process and methods can vary by organization
- There are ambiguities in every TARA process and approach
- Artifacts and deliverables can be organized in different ways and contain different information
- TARAs, by their nature, are very subjective and experience matters
- There is a lot of room for variation across large organizations with multiple product groups and varying levels of competence
- How to ensure TARA is a “living document” is not included in any of the guides

ORGANIZATIONAL STRUCTURE

DIFFERENT APPROACHES

ORGANIZATIONAL STRUCTURE

- **Distributed**
  - Engineers at the component/product level perform the TARA function
    - May or may not include cybersecurity training or certification
  - Specialized cybersecurity staff assigned to the component/product team perform the TARA function
- **Centralized**
  - Centralized team, develops and maintains TARAs for the entire organization, and works on multiple components/products at a time
- **Disorganized**
  - Organization is in the early phase of incorporating TARA into the development lifecycle, and no formal organizational structures exist

ORGANIZATIONAL STRUCTURE

- There are many different approaches being employed to review output and ensure quality assurance
- In the best cases, there was peer review followed by senior expert and management review and sign-off
- In the worst cases, there were few, if any, peer or formal review processes
- There is no guidance on developing a quality TARA process in any of the supporting documentation
- Best practice quality assurance business process methods are not always applied in cybersecurity environments

ORGANIZATIONAL STRUCTURE

- The amount of time taken to complete a TARA depends significantly on whom is doing the work
- External cybersecurity professionals take about 4 to 8 weeks for a TARA, depending on the size and complexity of item
- Internal staff take about 2 to 4 weeks to complete a TARA
- Internal staff have the benefit of inside knowledge, and external professionals tend to take a deeper dive and consider more attack paths and scenarios
- Most organizations perform TARAs internally, but a few engage external experts for more complex items

SUPPLY CHAIN OBSERVATIONS

PERSPECTIVES

OEM OBSERVATIONS

- TARA process maturity varies substantially across OEMs, even the big ones
- TARAs are not always used in conjunction with ISO/SAE 21434
- Supplier agreement maturity varies significantly between OEMs
- The most significant variations or issues seem to be incorporating TARA information from and with suppliers (SBOM/HBOM)
- Most have a regulatory group that interacts with regulatory authorities for R155 type approval, either lawyers, engineers, or a mix of both.
- People who create and maintain TARA rarely ever interact with regulatory authority

TIER 1 SUPPLIER OBSERVATIONS

- Great variance in maturity between various Tier1 suppliers
- Tier1 suppliers tended to be less mature than the OEMs, but not always
- Some are ISO/SAE 21434 “compliant,” but many are not since they only supply parts
- Some Tier1 suppliers have supplier interface agreements, but many do not; instead, they use more traditional supplier agreements
- SBOMs and HBOMs are starting to become prevalent

INDUSTRY EXPERT OBSERVATIONS

- TARAs take longer and cost more than the client thinks they should
  - Lack of item or product documentation
  - Explore more attack paths than an internal team
  - Have a well-documented and specific process and deliverable templates to produce consistent and high-quality results
  - Processes are usually more comprehensive due to experience in multiple types of embedded systems
  - Extensive knowledge of vulnerabilities and cutting-edge hacking techniques
- Performing a thorough and high-quality TARA is laborious and tedious work, which causes project staffing challenges

TOOL PROVIDER OBSERVATIONS

- Majority of prospective customers use spreadsheets
- Fighting for budget is still an issue
- EU market is showing higher motivation than US market due to R155
- US and Asian markets are proving more difficult
- Tool providers is only group that mentioned Auto-ISAC threat matrix

TOOL PROVIDER OBSERVATIONS

- Integration with existing engineering processes with unique tool chains is an ongoing learning experience for everyone
- Focus on moving to dynamic environments for “living documents”
- Large item definitions yield large spreadsheets with too much complexity
- Features include dashboards, automated attack trees, reports, alerts, and many other features to manage complexity across enterprise

TOOL PROVIDER OBSERVATIONS

- Provide integration with SBOM/HBOM and reported vulnerabilities
- Integrating direct support for UNECE R155 Annex 5 – *List of threats and corresponding mitigations*
- Looking at advanced solutions like direct Ghidra support, which seems bleeding edge
- Functionality across vendors varies, and customers should consider all major vendors to find best fit for organization

REGULATORY AUTHORITY OBSERVATIONS

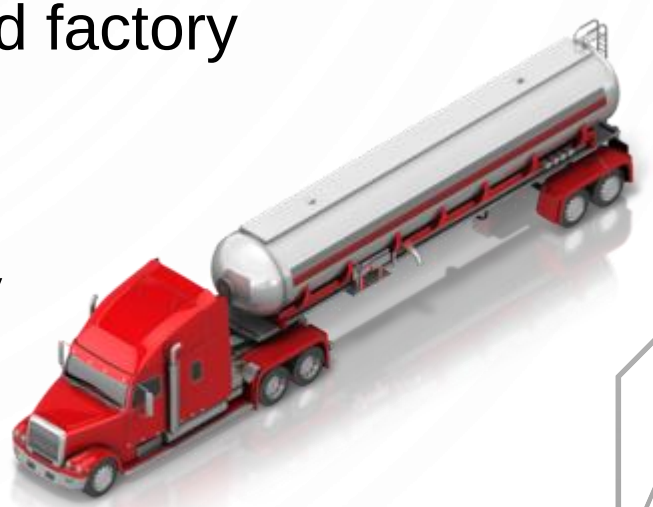
- First priority is to evaluate company processes Cyber Security Management System (CSMS)
- Review TARA process and validate TARA output
- Check to ensure the risk profile is maintained over time
- TARA must be a living document
- Challenges with incremental changes as there are no set rules of when a new type certification is required
- Heavy Vehicle type certifications are complicated by the flexibility of vehicle configuration. Focus on most complex configuration.
- Try to tailor the approach based on product and type

REGULATORY AUTHORITY OBSERVATIONS

- Issues observed by the authority
  - Over classification -> impact too high
  - Only looking at Annex 5 -> scope should be broader
  - TARA is subjective, resulting in varied quality
  - Tools vs Excel spreadsheets -> Regulator/audit access
- Review CSMS every 3 years or so
- Tweak type approvals for type extensions
- Looking for updated TARAs when looking at extensions
- Looking for risk management, i.e. mitigated, transferred, accepted
- At the end of the day, it is about handling risk

TRUCKING FLEET OBSERVATIONS

- Most commercial fleets are only marginally aware of ISO/SAE 21434 or similar standards or regulations, such as UNECE R155 and R156
- Cybersecurity awareness and posture vary significantly across the industry and types of fleets
- Assessment at vehicle build stage through paper and factory pilots, and 2nd market evaluations.
- TARAs could be useful, but are not employed
- Heavy Vehicle OEM customer education opportunity



COMMON ISSUES

COMMON ISSUES

- TARA consistency seem to be a common issue across the supply chain
  - A factor of processes, assumptions, and deliverables
  - Lack of scaffolding, i.e., process documentation, templates, etc.
- TARA accuracy, especially impact assessments, also seems to be common issue across the entire ecosystem
  - Assumptions, experience, and cybersecurity “know-how”
- Mixed tool and manual documentation
- Little or no document management support or document management systems in place

COMMON ISSUES

- Varying levels of training and expertise
- Little or no documentation or examples
- Sharing TARA information across the supply chain from “Tier n” to the regulatory authority seems challenging
- Mismatch and inexperience in supplier interface agreements
- New technologies such as EVs cause additional supplier agreement and interface agreement issues

CONCLUSION

SAFETY-CRITICAL PROCESS OR CHECK BOX COMPLIANCE?

CONCLUSION

- There are many ways that TARAs can be implemented and supported
- Not everyone is using ISO/SAE 21434 to meet R155 compliance, but some still use TARAs as part of the development lifecycle
- TARAs are mostly taken seriously as part of safety-critical systems
- A few minor suppliers consider it to be check-box compliance because they have little to no connectivity
- Adoption and integration of TARAs is a journey that is specific to the company and process should be reviewed and updated regularly
- Everyone seems to have issues with quality and consistency

HOW TO IMPROVE

HOW TO IMPROVE

- Review existing processes
- Empower the person conducting TARA
- Support person conducting TARA
  - Process documentation with complex and robust examples
  - Tools and document management systems
- Implement quality control processes and criteria
- Improve training across the organization, including engineering, purchasing, legal, etc.
  - Training providers exist, including SAE and UL/Kugler-Maag
- Get process metrics - *“if you can’t measure it, you can’t improve it”*

PROCESS IMPROVEMENT

BPR, BPM, BPMN, LEAN, SIX SIGMA, VALUE STREAM MAPPING, ETC.

PROCESS IMPROVEMENT

- **Identify the process**
- **Map the current process**
  - Business process model and notation (BPMN)
- **Analyze the process**
  - Root cause analysis, value add vs not, cycle time, and wait time tracking
  - Define key performance indicators (KPIs) to measure the process
  - Determine error rates, rework, tasks, and effort at each stage of the process
- **Identify possible improvements**
  - Eliminate waste, simplify hand-offs and approvals, standardize tasks
  - Add automation and tool support

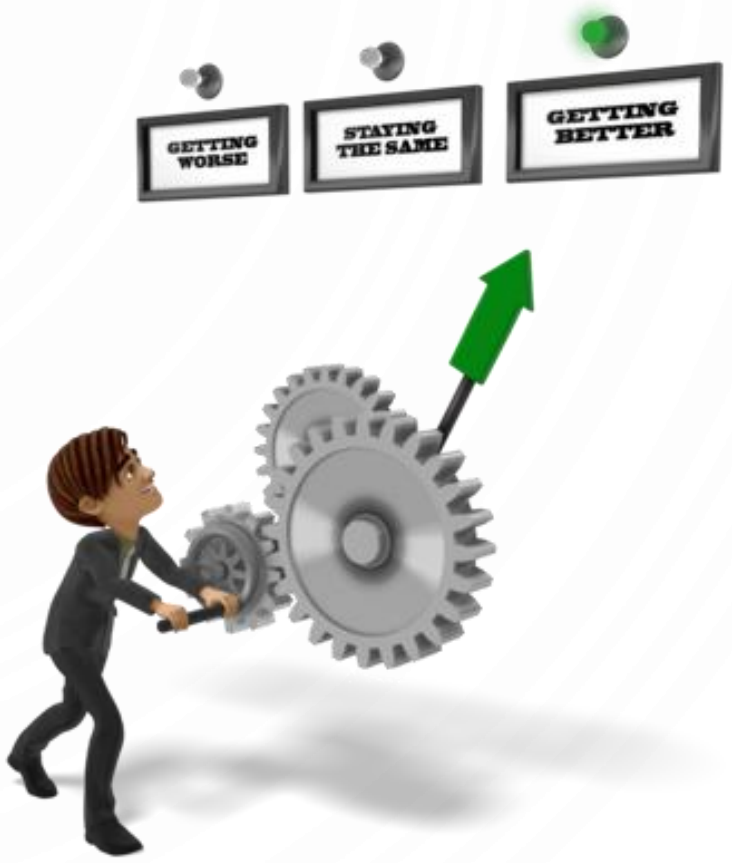
PROCESS IMPROVEMENT

- **Design future state**
  - Improved process map with new workflow
  - Add controls, automation, and update roles
  - Ensure goals align with business goals
- **Validate and test the new process**
  - Simulate or pilot with a small group
  - Collect feedback and update the new business process design
- **Implement and monitor**
  - Roll out the new process across the organization
  - Use key performance indicators (KPIs), i.e. metrics to measure results
- **Continuous improvement**
  - Monitor KPIs and adjust accordingly to continue to improve over time

30,000 FT VIEW

WHAT IS THIS AT A HIGH LEVEL?

- Process improvement
- Can lead to
  - Reduction in costs and expenses
  - Improved turnaround time
  - Higher quality and greater consistency
- Not limited to TARA
- Process improvement can be applied anywhere
  - Cybersecurity
  - Information Technology (IT)
  - Operational technology (OT)



MANAGEMENT ISSUES

- Return On Spend (ROS)
- Return On Security Investment (ROSI)
- How much is something costing you?
- Are you getting a good return on your spend?
- Organizations, departments, and processes usually develop organically, which is usually not optimal
- Best practices process review and engineering require an outside perspective
  - “That’s the way we’ve always done it”

INDUSTRY DEVELOPMENTS

INDUSTRY DEVELOPMENTS

- Updates to ISO/SAE 21434 starting work in 2026
- New Chinese Standards
  - GB 44495 and GB 44496
  - Similar to UNECE WP.29 R155 and R156
  - Specific requirements
  - Additional specific tests and scenarios
- SAE J3334 – TARA Guidelines (WIP)
  - Threat Analysis and Risk Assessment (TARA) Task Force
  - SAE TEVEES18A5
  - Chad Childers, Chris Lupini, Luis Molleda

WRAP-UP

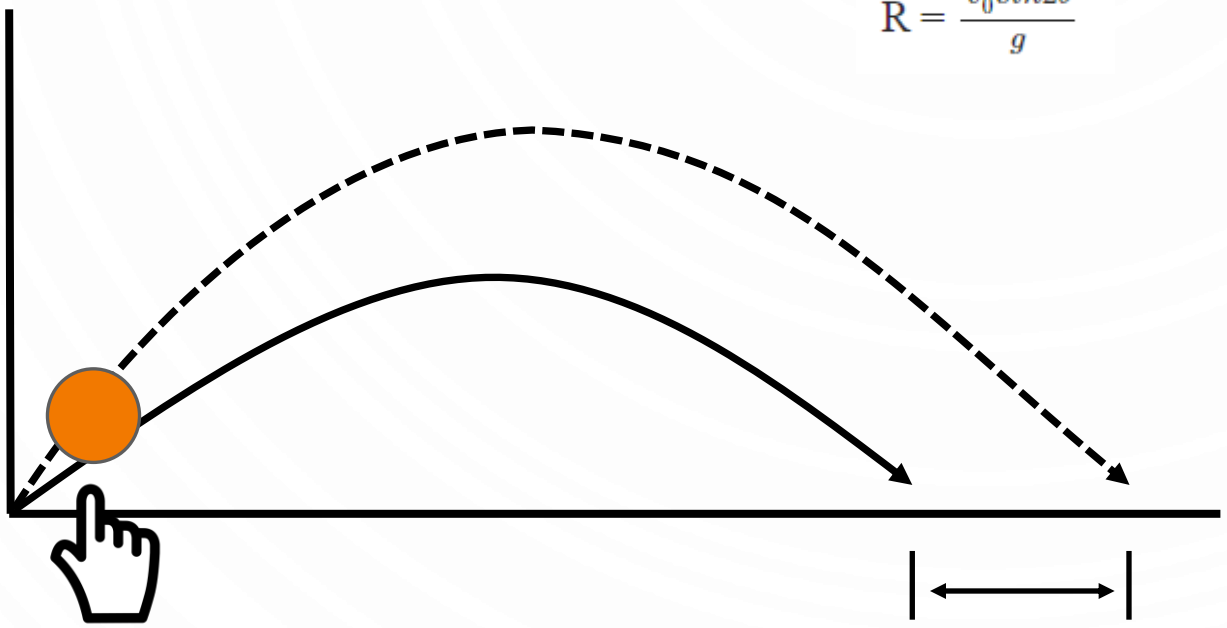
AGENDA

- Why this topic?
- Threat Analysis and Risk Assessment (TARA) Overview
- Organizational Structure
- Supply Chain Observations
- Common Issues
- Conclusions
- How to Improve
- Process Improvement
- 30,000 ft View
- Industry Developments

SMALL CHANGES CAN HAVE A BIG IMPACT

Horizontal Range

$$R = \frac{v_0^2 sin2\theta}{g}$$

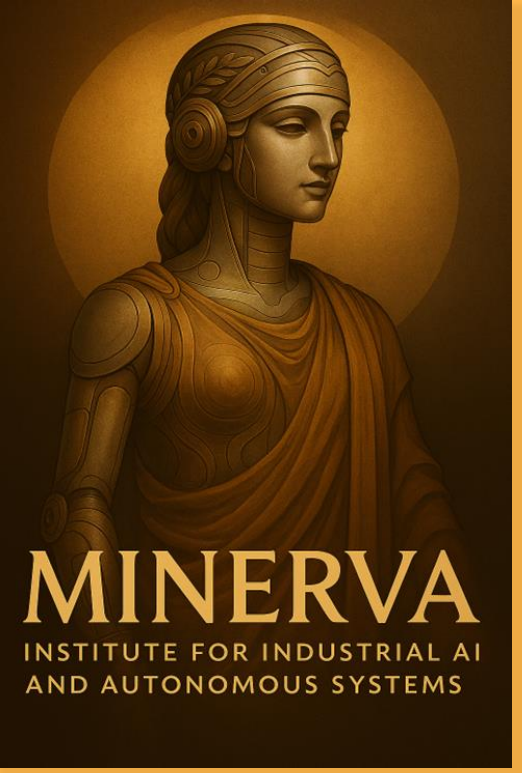


Trajectory

$$y = x \tan \theta - \frac{gx^2}{2{v_0}^2 cos^2\theta}$$

THANK YOU

Thank you to everyone who participated in developing this survey and research…



Mission

To guide and support industry and public institutions via research and education in the secure, strategic, and resilient integration of artificial intelligence and autonomous systems into industrial operations, processes, and infrastructure, including the critical sectors of energy, utilities, transportation, and manufacturing.

Policy Research: Advancing industrial AI and autonomy through actionable policy guidance.

Operational Resilience & Assurance: Safeguarding legacy and modernized control systems with AI-informed frameworks.

Technology Assessment, Forecasting, & Risk Reduction: Providing roadmap alignment for AI/autonomy over key horizons.

Standards and Best Practices: Co-creating scalable, interoperable industrial standards.

Ethical and Responsible Integration: Embedding human-in-the-loop safety and accountability.

Public-Private Collaboration: Connecting innovators with regulators and operators.

For More Information or To Become a Member, Contact Us At:

Ernest Wohnig
Executive Director
ewohnig@minervainstitute.ai

Urban Jonson
ujonson@minervainstitute.ai

Q&A

Urban Jonson

ujonson@serjon.com

www.serjon.com

Services

- Advisory Services
- Cybersecurity Training
- Industry Research
- Custom Threat Intelligence
- Threat and Risk Assessments
- Standards and Regulatory Gap Analysis

eLearning: learning.serjon.com
YouTube: https://www.youtube.com/@serjon14
Website: www.serjon.com
LinkedIn: https://www.linkedin.com/in/urban-jonson/

FURTHER INFORMATION

- **ISO/SAE 21434**, especially appendices
- **NIST SP 800-30** – Guide for Conducting Risk Assessments
- **Managing Cybersecurity Risks Using ISO/SAE 21434** (https://www.sae.org/learn/content/pd532013/)
- Brook S. E. Schoenfield. 2015. **Securing Systems: Applied Security Architecture and Threat Models**. CRC Press, Inc., USA.
- Ivar Jacobson, Maria Ericsson, and Agneta Jacobson. 1994. **The object advantage: business process reengineering with object technology**. ACM Press/Addison-Wesley Publishing Co., USA.