AXIS / Technology

Practical Guidance

From Prototype to Production: The New Risk Landscape in Advanced Manufacturing

Why advanced manufacturing companies need a risk strategy before commercialization.

Written by Tristan Smith

Advanced manufacturing companies are moving rapidly from R&D and pilot environments into commercial deployment. Robotics, AI-enabled systems, industrial automation, connected manufacturing, advanced materials, quantum technologies, and digitally integrated production environments are creating new opportunities, but also new forms of operational, contractual, cyber, and intellectual property risk.

As technologies scale, the risk profile changes materially. A failure that once affected a controlled pilot can now disrupt customer operations, trigger contractual liability, create cyber-physical loss, expose supply chain dependencies, or lead to intellectual property disputes.

For manufacturers, technology developers, investors, and commercialization partners, the question is no longer simply whether the technology works. It has shifted to whether the organization is prepared for the financial and operational consequences if something goes wrong.

Why Commercialization Changes the Risk Profile

Advanced manufacturing projects often begin as technical collaborations. As they scale, they become commercial obligations.

That shift creates new exposure across contracts, intellectual property, product performance, cyber resilience, supply chains, and customer commitments. A technology that performs well in a pilot can still create significant financial loss if it fails in a customer environment, delays production, triggers a recall, infringes third-party IP, or exposes operational systems to cyber disruption.

For manufacturers, technology developers, investors, and project partners, the key question is not only whether the project can be built. It is whether the business can absorb the consequences if the project fails, is delayed, or becomes the subject of a dispute.

Five Risk Areas to Review Before Scaling

1. Intellectual Property Ownership and Infringement

Collaborative projects can blur the line between background IP, newly created IP, licensed technology, trade secrets, software, data, and manufacturing know-how.

Before commercialization, project partners should clearly define:

- Who owns existing IP brought into the project;
- Who owns new IP developed during the project;
- Who has the right to commercialize, license, or modify the technology;
- Who is responsible if a third party alleges infringement; and
- Whether indemnity obligations are backed by insurance.

This is especially important because Technology E&O policies often provide limited protection for IP disputes, particularly patent infringement or offensive enforcement actions. Dedicated IP insurance can help protect against infringement defense costs, contractual IP indemnities, pursuit of infringers, title disputes, invalidation challenges, and loss of future profit where applicable.

2. Contractual Indemnities and Customer Obligations

As advanced manufacturing companies move from funded development to commercial contracts, indemnity obligations often expand. Enterprise customers, strategic partners, and international buyers may require broad indemnities for IP infringement, product failure, confidentiality breaches, cybersecurity incidents, regulatory violations, or supply chain disruption.

The risk is that a company may agree to contractual obligations that exceed what its insurance policy was designed to cover.

Before signing, companies should review whether indemnity wording aligns with available coverage. Poorly drafted clauses can trigger contractual liability exclusions, create uninsured defense obligations, or require one party to assume responsibility for losses caused by another. Well-drafted indemnities should be tied to the party's own acts or omissions, preserve defense control, and align with the policy wording that must respond.

3. Product Liability, Technology E&O, and Recall Exposure

Advanced manufacturing often combines software, hardware, automation, robotics, AI, materials science, and process engineering. That creates a coverage challenge because a single failure can trigger multiple policies.

For example:

- A robotics system fails and damages customer equipment;
- An AI-enabled quality control tool misses a defect;
- A battery component causes downstream product failure;
- A manufacturing process delays customer production;
- A satellite or quantum component does not perform as contracted; or
- A healthcare manufacturing technology creates patient or regulatory exposure.

Some losses may fall under Product Liability. Others may fall under Technology E&O. Some may require Product Recall, Professional Liability, Cyber, or specialized coverage. Companies should not assume one policy will respond to every advanced manufacturing failure.

4. Cyber, OT, and Connected Factory Risk

Advanced manufacturing is increasingly connected. Industrial AI, digital twins, robotics, automated production lines, cloud-connected equipment, and smart sensors improve efficiency, but they also increase cyber and operational technology exposure.

A cyber incident in a connected manufacturing environment can create more than data loss. It can cause production downtime, physical process disruption, defective output, contractual penalties, customer losses, safety concerns, and dependent business interruption.

Cyber coverage should be reviewed for:

- Business interruption and contingent business interruption;
- System failure and non-malicious outage;
- Cyber-physical loss;
- Data restoration and recreation;
- Ransomware and extortion response;
- Social engineering and funds transfer loss;
- Vendor-caused incidents; and
- War, infrastructure, or state-backed cyber exclusions.

This is especially important where manufacturers rely on AI-enabled systems, cloud platforms, or third-party technology providers. Policy silence can create uncertainty when AI is the cause, vector, or trigger of a loss.

5. Vendor, Subcontractor, and Supply Chain Risk

Many advanced manufacturing projects depend on specialized vendors, research partners, contract manufacturers, component suppliers, cloud providers, testing labs, and distribution partners.

Every partner creates a potential point of failure. A weak supplier, insecure vendor, late component, untested subcontractor, or financially unstable partner can delay commercialization and create losses that flow back to the lead company.

A practical vendor onboarding process should include:

- Pre-engagement due diligence;
- Security and compliance verification;
- Clear contractual risk allocation;
- Insurance requirements and evidence of coverage;
- Access control and data segmentation;
- Ongoing monitoring; and
- Incident reporting obligations.

Insurers increasingly view vendor governance as a sign of operational maturity. A documented onboarding process can support better underwriting outcomes and reduce the likelihood of coverage disputes after a third-party failure.

What Will Insurers Ask?

As public funding accelerates commercialization, insurers will expect companies to demonstrate control over how risk is managed. Strong submissions should answer the following questions:

1. **What is being manufactured, and where will it be used?**
   Insurers need to understand whether the product is used in industrial, healthcare, energy, aerospace, defence, consumer, or critical infrastructure settings.
2. **How is the supply chain structured, and how is risk transferred?**
   Insurers will review where components and software are sourced, including single-source dependencies. They will evaluate how vendor contracts, indemnities, and quality control protocols transfer or mitigate operational risks.
3. **What contracts govern the project?**
   Funding agreements, consortium agreements, supplier contracts, customer MSAs, licensing agreements, and distribution agreements should be reviewed for indemnities, liability caps, warranties, insurance requirements, and dispute resolution.
4. **What could go wrong in a real customer environment?**
   Scenario testing should consider product failure, customer downtime, recall, bodily injury, property damage, IP infringement, cyber disruption, and supply chain delay.
5. **What controls are in place?**
   Insurers will look for quality management, testing protocols, traceability, cyber controls, vendor oversight, employee training, incident response planning, and documented governance.

.

Best Practices

1. Review contracts before execution

Do not wait until after funding is awarded or a customer contract is signed. Review indemnities, liability caps, warranties, insurance requirements, IP ownership, and defense obligations before commitments become binding.

2. Match coverage to the commercial use case

A pilot project and a commercial deployment do not carry the same risk. Coverage should be reviewed once the technology moves into customer environments, international markets, regulated sectors, or safety-critical applications.

3. Build insurance into consortium and partner agreements

Every project partner should carry appropriate insurance for its role. Contracts should require evidence of coverage, notice of cancellation, indemnity alignment, and clear allocation of responsibility for IP, cyber, product, and operational failures.

4. Stress-test limits against realistic loss scenarios

Selecting limits should not be based only on premium affordability. Limits should be tested against potential customer losses, recall costs, contractual indemnities, U.S. or EU litigation exposure, cyber downtime, and the company's balance sheet capacity.

5. Review exclusions carefully

Advanced manufacturing companies should pay close attention to exclusions or limitations involving patents, contractual liability, product recall, professional services, cyber-physical loss, AI-enabled decision-making, pollution, regulatory fines, liquidated damages, and war or state-backed cyber events.

6. Complete a structured risk assessment

Companies can also use the Axis Risk Compass assessment at https://axisinsurance.ca/commercial-insurance/axis-technology-risk-compass/ to help identify control gaps, organize risk information, and prepare a stronger underwriting submission. The assessment is designed to map risk controls, provide a Compass Score and report, and support underwriting-ready positioning.

Takeaway

Public funding can help validate a technology. It does not transfer the financial risk of commercialization.

As Canadian advanced manufacturing companies move from research to production, their insurance programs must evolve at the same pace. The risks are no longer limited to the lab. They now sit in customer contracts, global supply chains, IP ownership structures, connected production systems, and product performance obligations.

Companies that align contracts, governance, and insurance before scaling will be better positioned to win customers, attract investment, satisfy funders, and recover when losses occur.

Before commercialization accelerates, review whether your insurance program is built for the obligations your project is about to create.

Contact us for guidance on aligning advanced manufacturing contracts, IP rights, cyber controls, and insurance coverage with your commercialization strategy.

Contact Us

Chris Jones
Account Executive,
Mining & Technology
+1 (778) 788-2853
Chris.Jones@axisinsurance.ca

Clive Bird
Senior Vice President,
Mining & Technology
+1 (604) 817-8072
Clive.Bird@axisinsurance.ca

Stacey Copeland
Vice President,
Mining & Technology
+1 (604) 619-7775
Stacey.Copeland@axisinsurance.ca

Tristan Smith
Business Development Specialist,
Mining & Technology
+1 (416) 885-0671
Tristan.Smith@axisinsurance.ca

About

Axis Insurance - Safeguarding the Exceptional. Axis Insurance is your strategic advantage; we cut through the complexity of risk management enabling you to confidently embrace the opportunities of tomorrow. Our role is to provide you with the best insurance value that combines coverage, service and price. We also provide personalized, quality service that includes professional insurance advice, ongoing policy maintenance and claims support. When any issue arises regarding your insurance coverage, we are your advocate, using our professional experience to best represent your individual interest. Follow Axis on LinkedIn, X, Facebook and Instagram. Stay up to date by signing up for our newsletter here.

axisinsurance.ca
#2000 – 1055 Dunsmuir Street, Box 49264, Vancouver, B.C. V7X 1L2
1-800-690-7475