

Strategic Application of Industry 4.0 Technology



Clive Milham

National Technology Adviser – Industry 4.0
Entrepreneurs' Programme



Australian Government
Department of Industry,
Innovation and Science



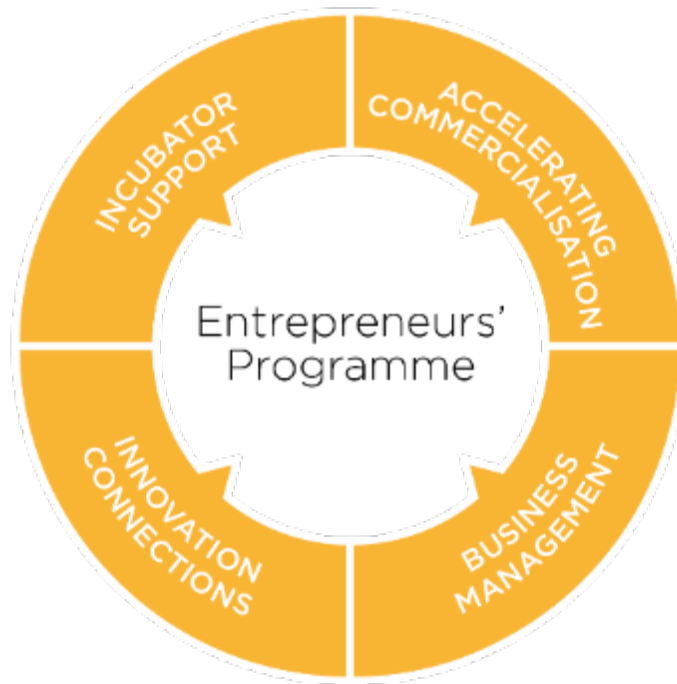
WEA Conference 2019

Entrepreneurs' Programme



Australian Government
Department of Industry,
Innovation and Science

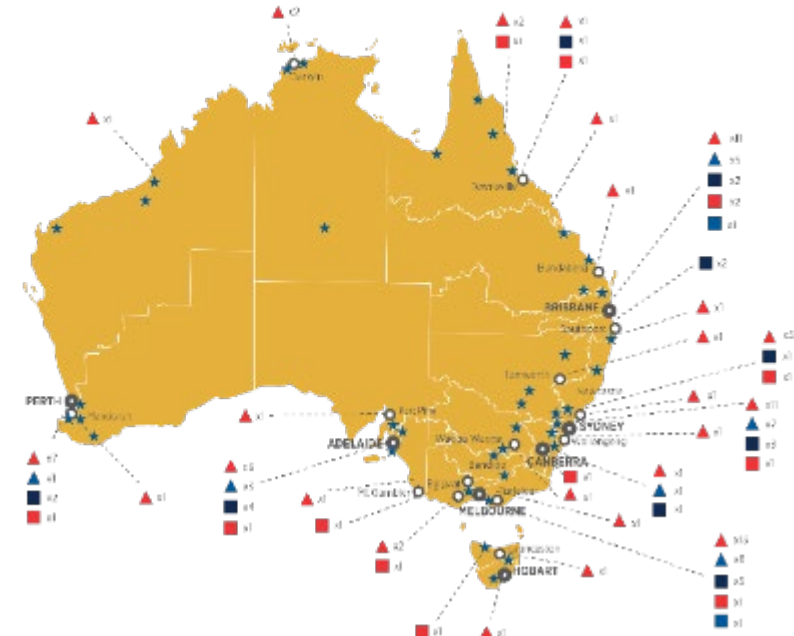
- Tailored and targeted advice and services to support small and medium (SME) businesses, entrepreneurs, incubators and researchers, including grant programs
- National network of 120 dedicated and industry experienced Advisors and Facilitators for Business, Innovation, Design and Commercialisation – holistic, impartial, unbiased



Australian Government
Department of Industry,
Innovation and Science
The Treasury

Business

STATE OFFICE	
●	National Office (entrepreneur, innovation, design, commercialisation)
▲	Business Adviser
■	Business Facilitator
▲	Commercialisation Adviser
■	Innovation Facilitator
■	Design Adviser
★	Australian Small Business Advisory Services



Australian Government
Department of Industry,
Innovation and Science

Business
Entrepreneurs' Programme

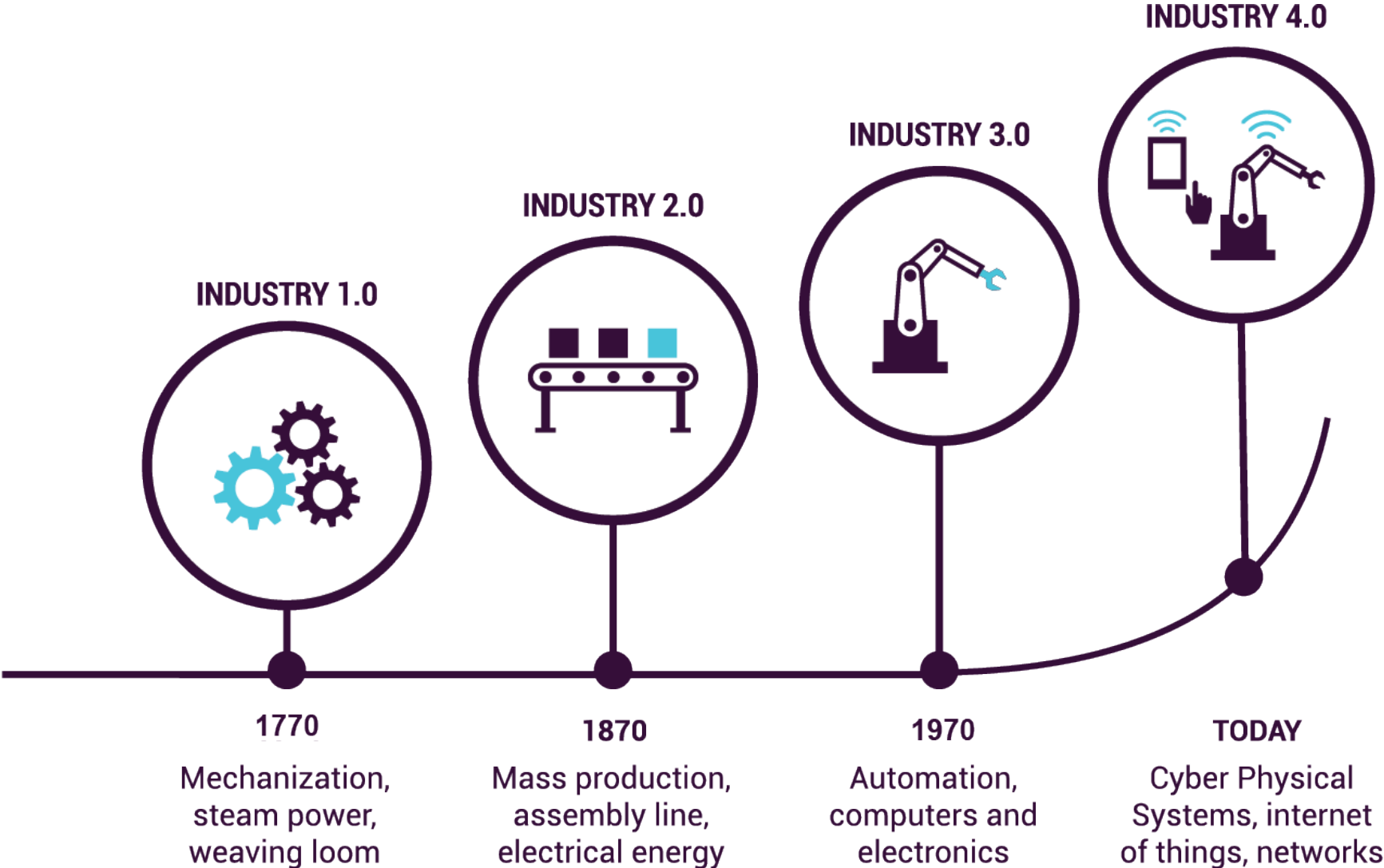


Presentation overview

- Industry 4.0
- Technology in action
- Opportunities for Industry 4.0 technology?
- Strategic application
- Getting started

Industry 4.0

The fourth industrial revolution





Federal Ministry
for Economic Affairs
and Energy

Federal Ministry
of Education
and Research

PLATTFORM
INDUSTRIE4.0



Industrie 4.0

In practice

About the platform

International cooperation



INDUSTRY 4.0

ADVANCED MANUFACTURING FORUM



Industry 4.0 Forum

Executive Council









Australia


work streams

Legal Framework


Reference Architecture Standards & Norms



Security of Networked Systems




Digital Business Models in Industry 4.0



Technology & Application Scenarios

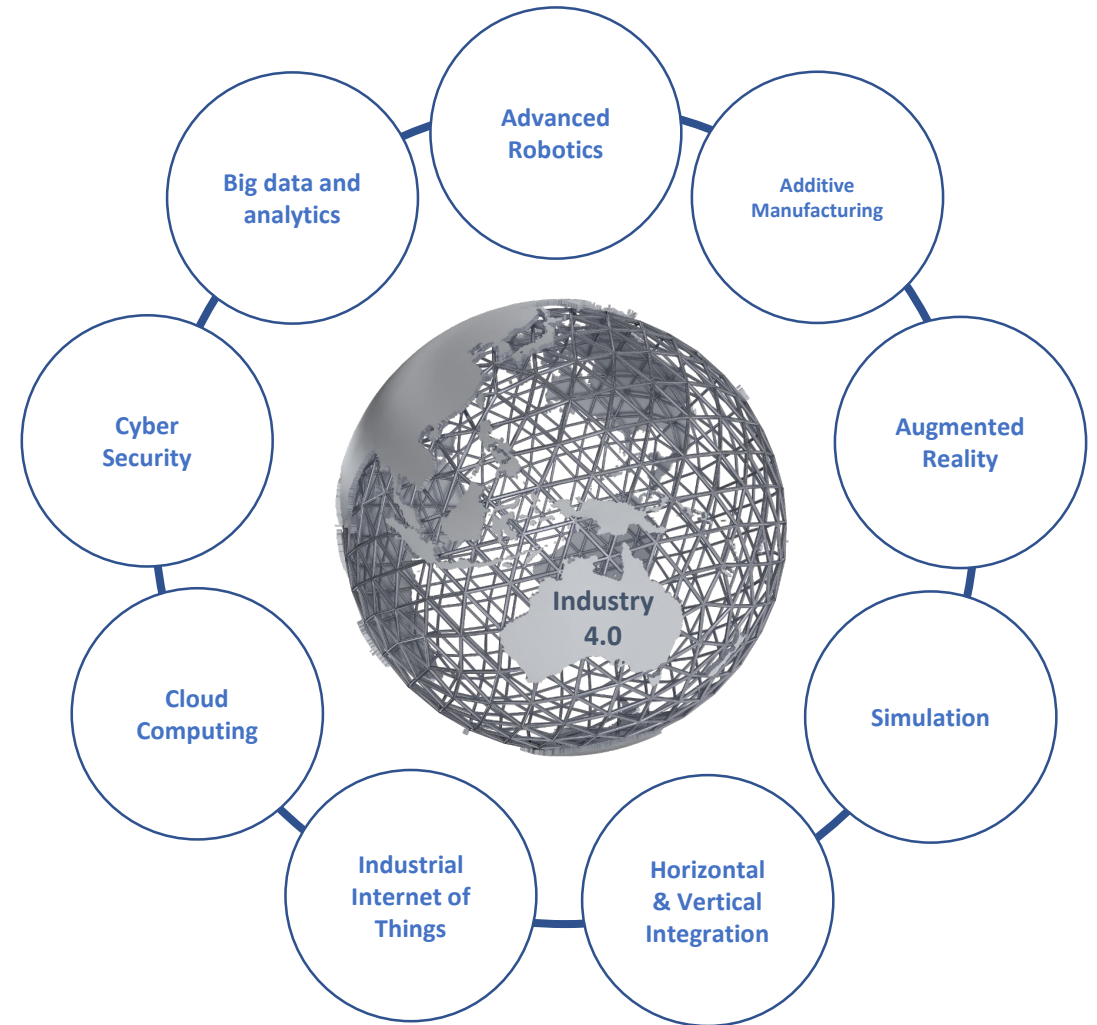
Work, Education & Training & Test Labs




PLATTFORM
INDUSTRIE4.0

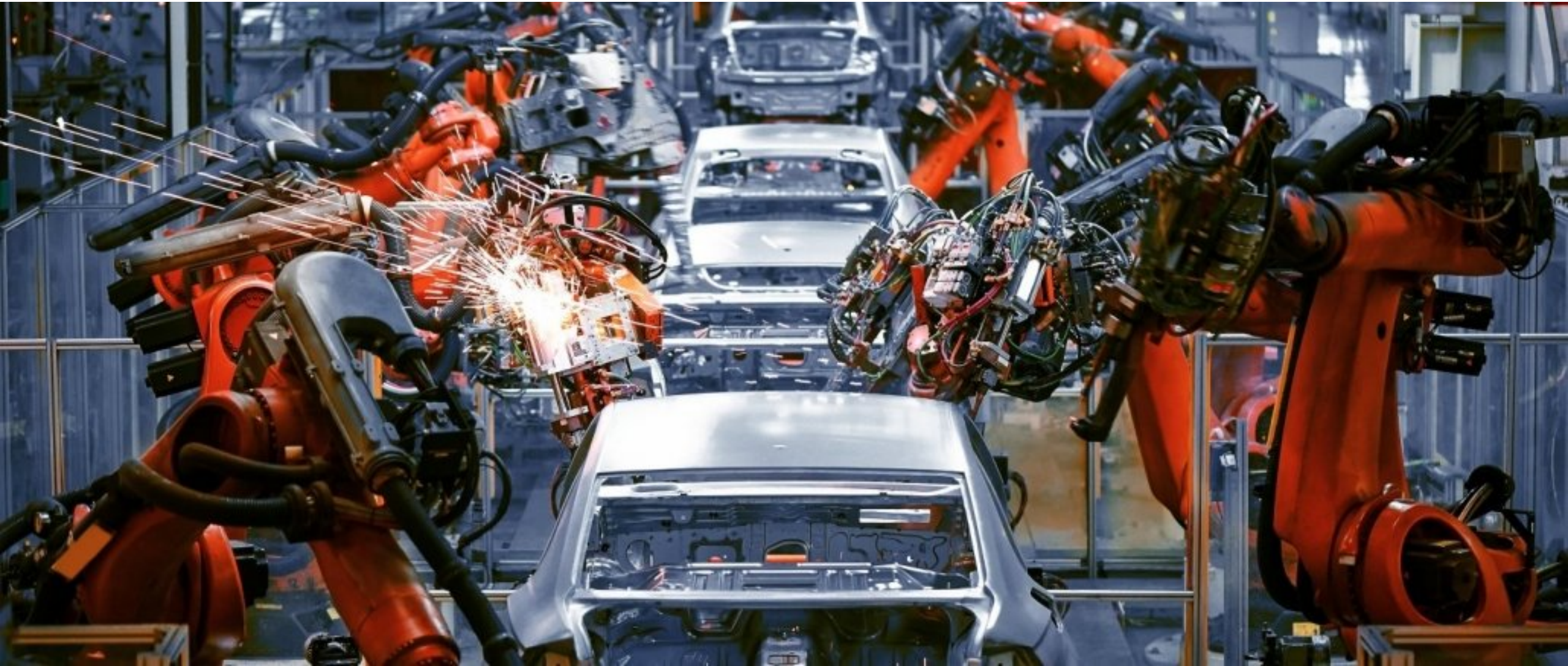
Industry 4.0 technology pillars

- Advanced Robotics
- Additive Manufacturing
- Augmented Reality
- Simulation
- Horizontal & vertical systems integration
- Industrial Internet of Things
- Cloud computing
- Cyber Security
- Big data and analytics

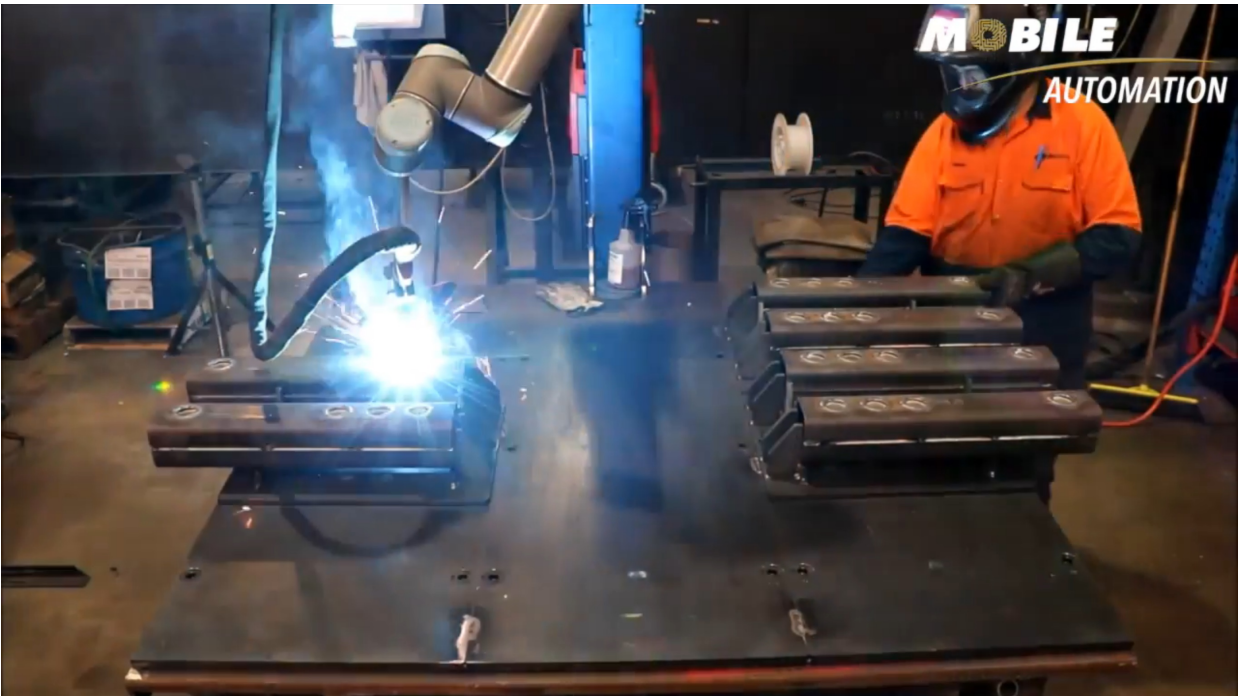


Technology in action

Advanced Robotics?



Collaborative Robotics



Mobile Robotics



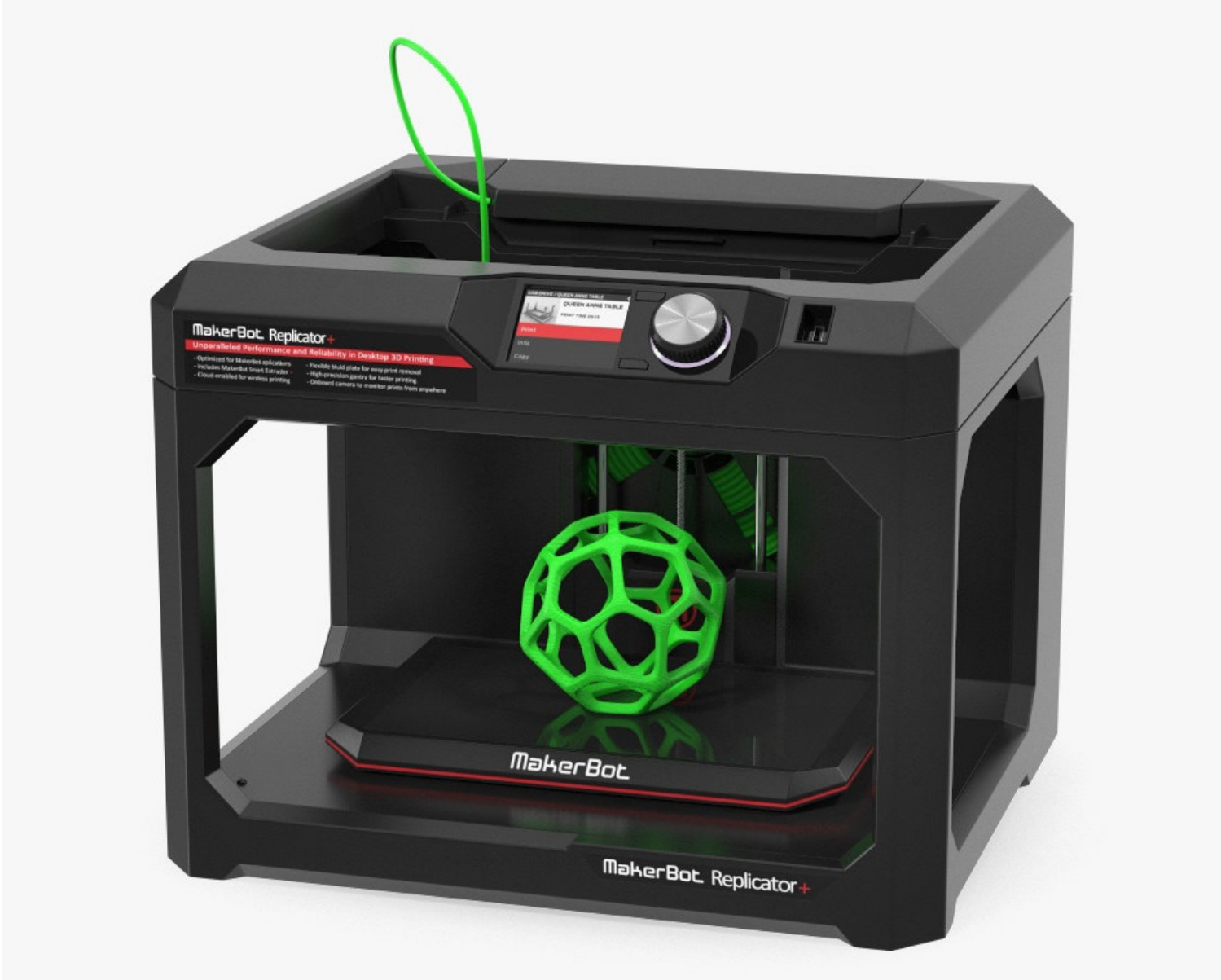
Field Robotics



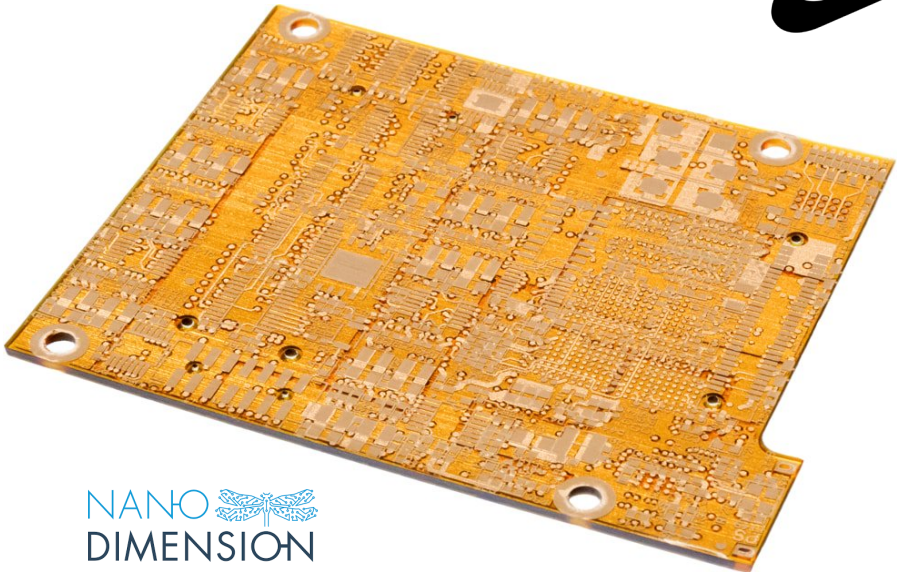
Australian Field Robotics



Additive Manufacturing



Additive Manufacturing



TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY 

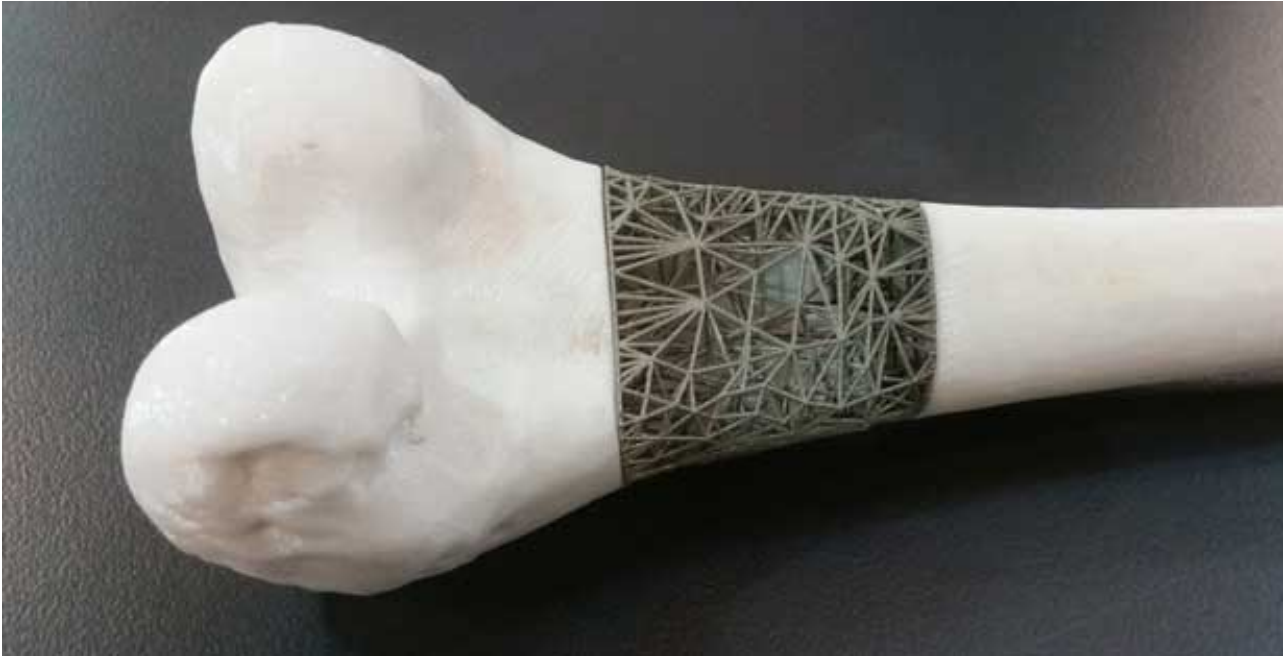
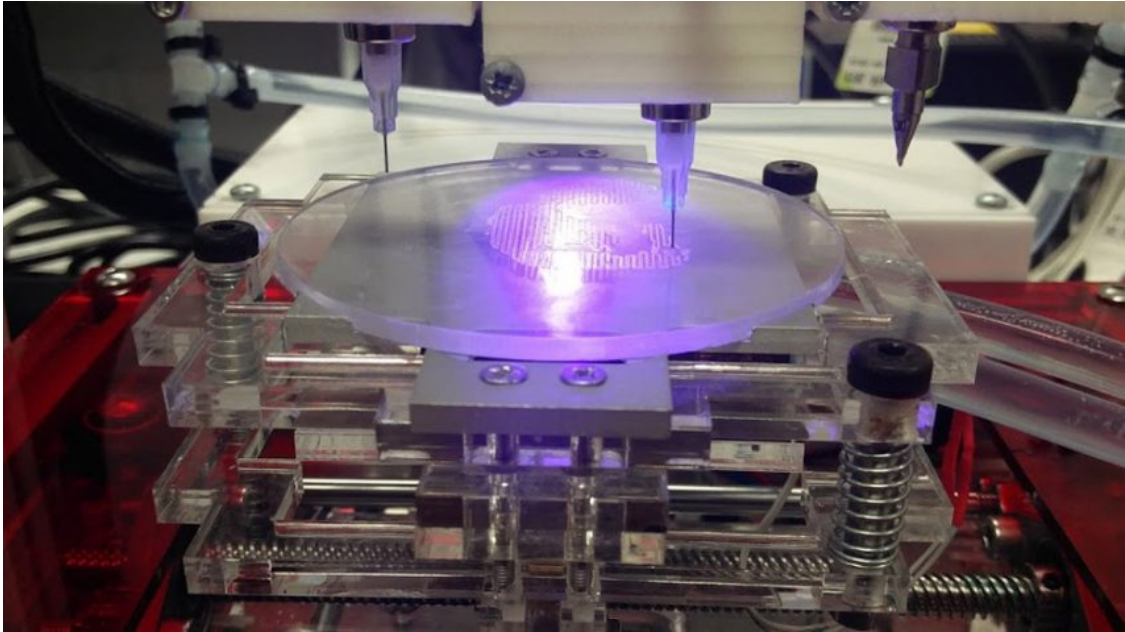
 Australian Government
Department of Industry,
Innovation and Science

Business
Entrepreneurs' Programme

NANO 
DIMENSION

Ai
GROUP

Additive Manufacturing



Additive Manufacturing



 **NORSK**
TITANIUM  **BOEING**



SIEMENS
Ingenuity for life

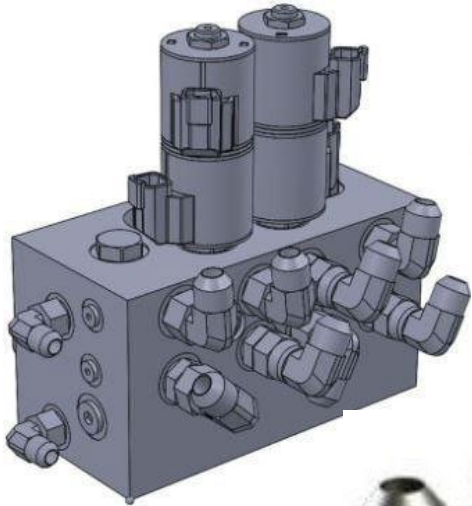


 Australian Government
Department of Industry,
Innovation and Science

Business
Entrepreneurs' Programme

 **BUGATTI**
 **SLM**
SOLUTIONS

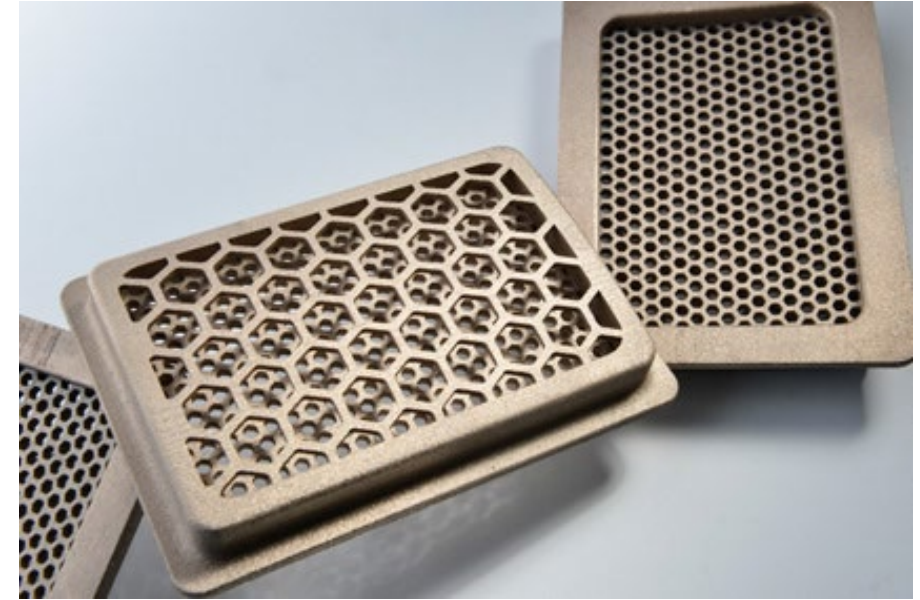
Additive Manufacturing



- ✓ Light weight (91%)
- ✓ Unitisation (13 → 1)
- ✓ Performance



Atlas Copco



Additive Manufacturing



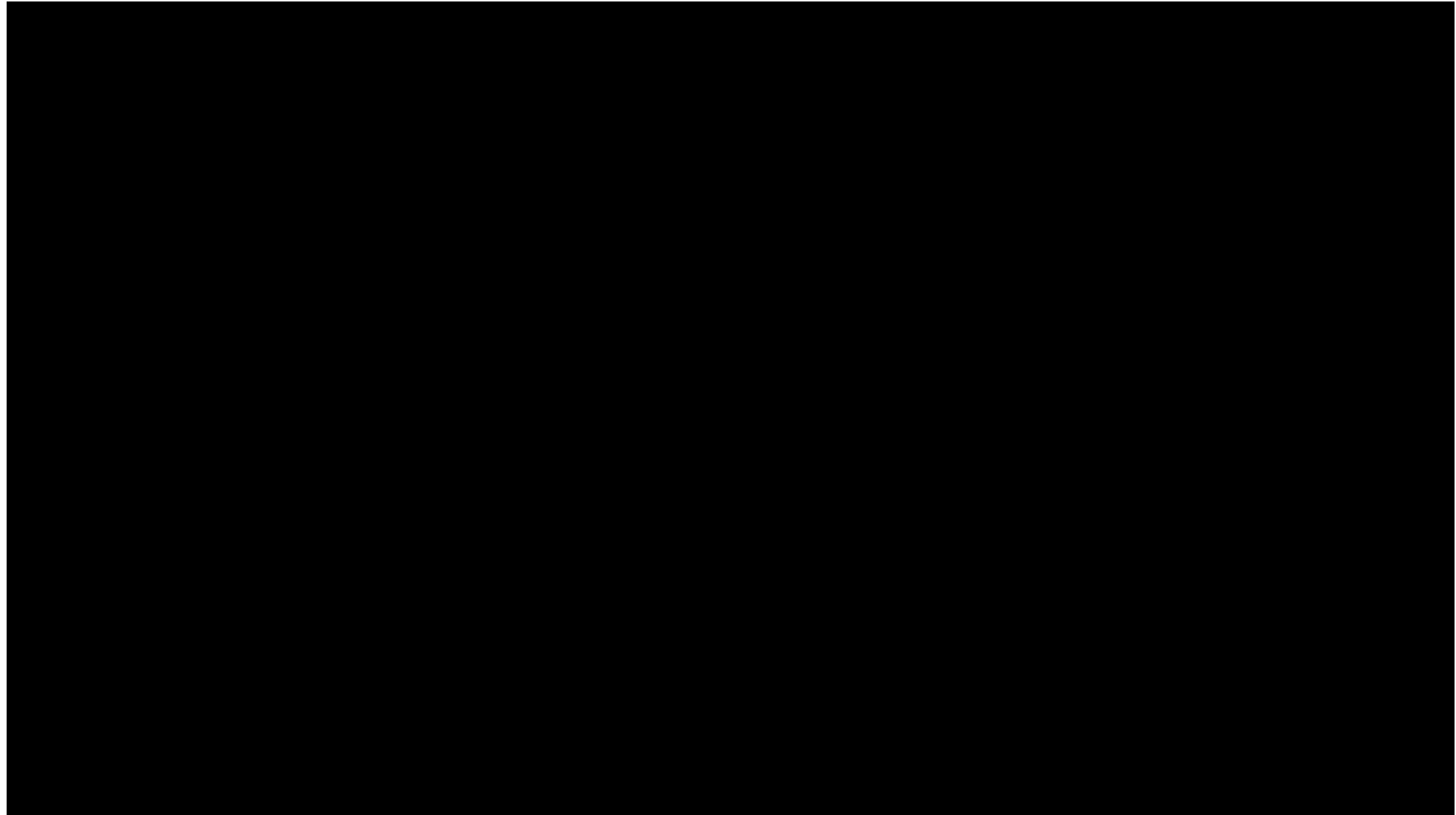


Hybrid Additive Manufacturing





Hybrid Additive Manufacturing

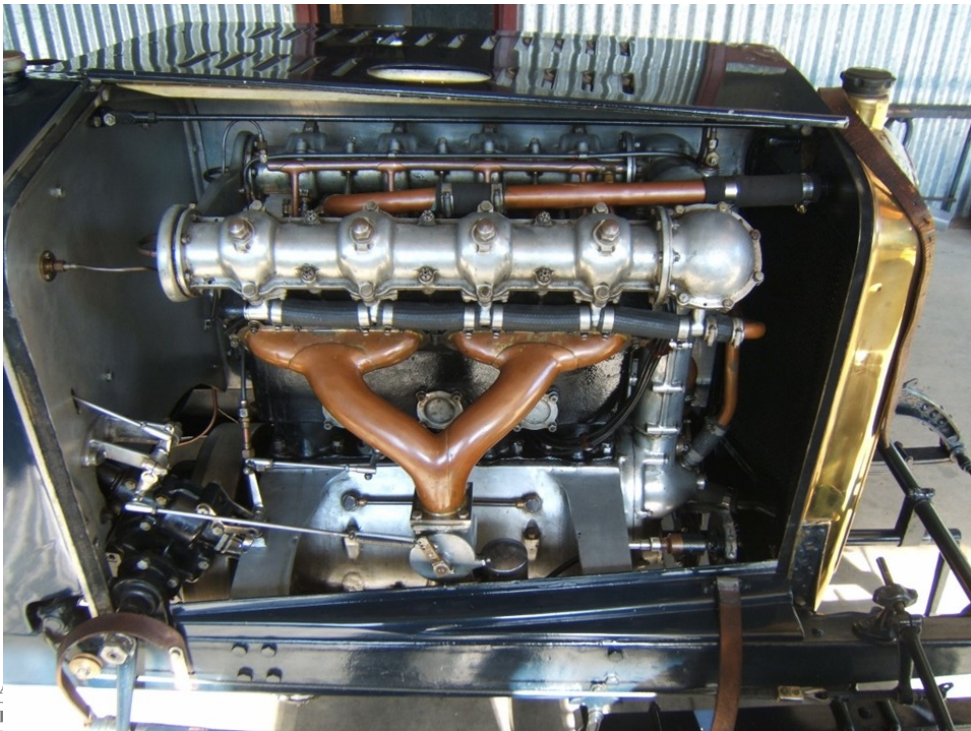
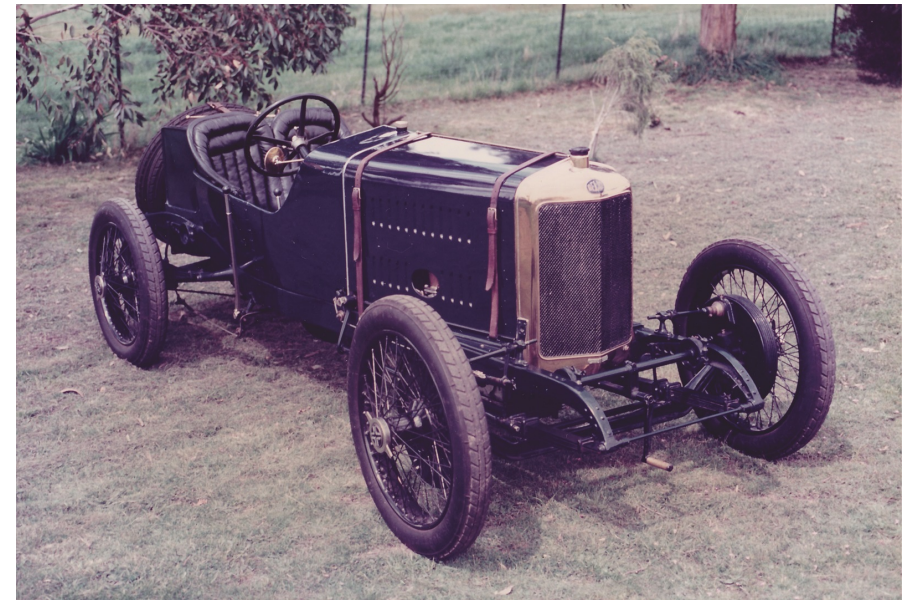


3D scanning

Additive manufacturing
pattern printing
- Investment casting



KEECH
A tradition of Innovation

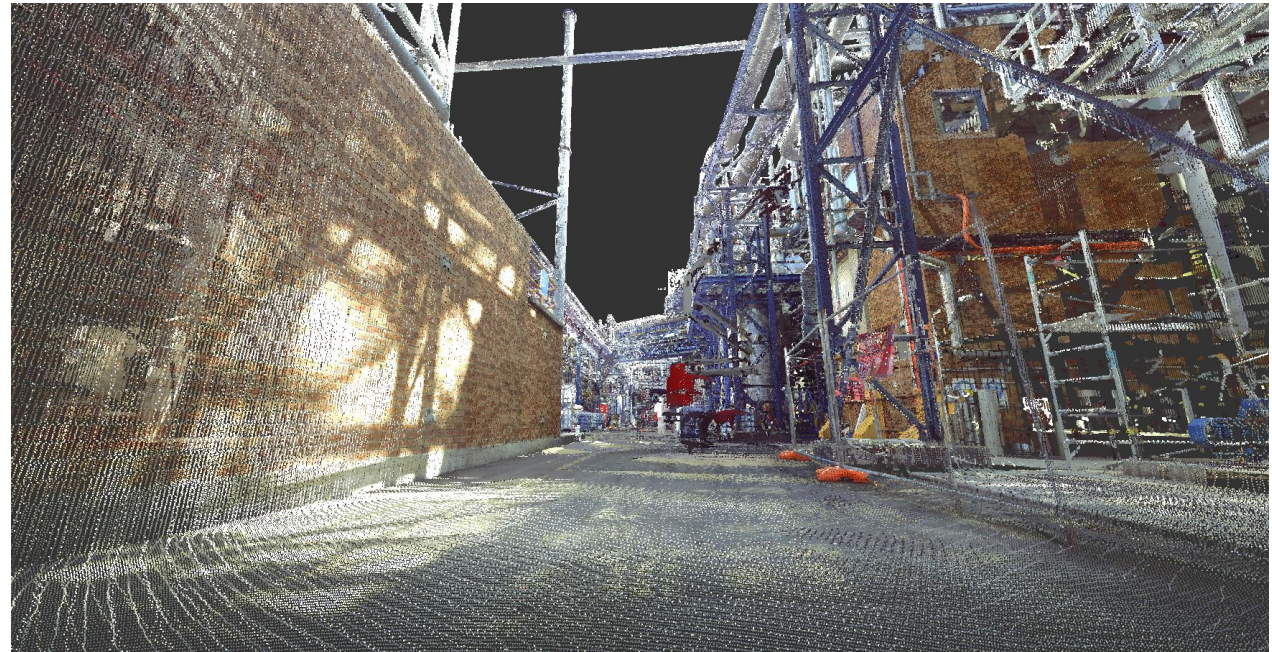
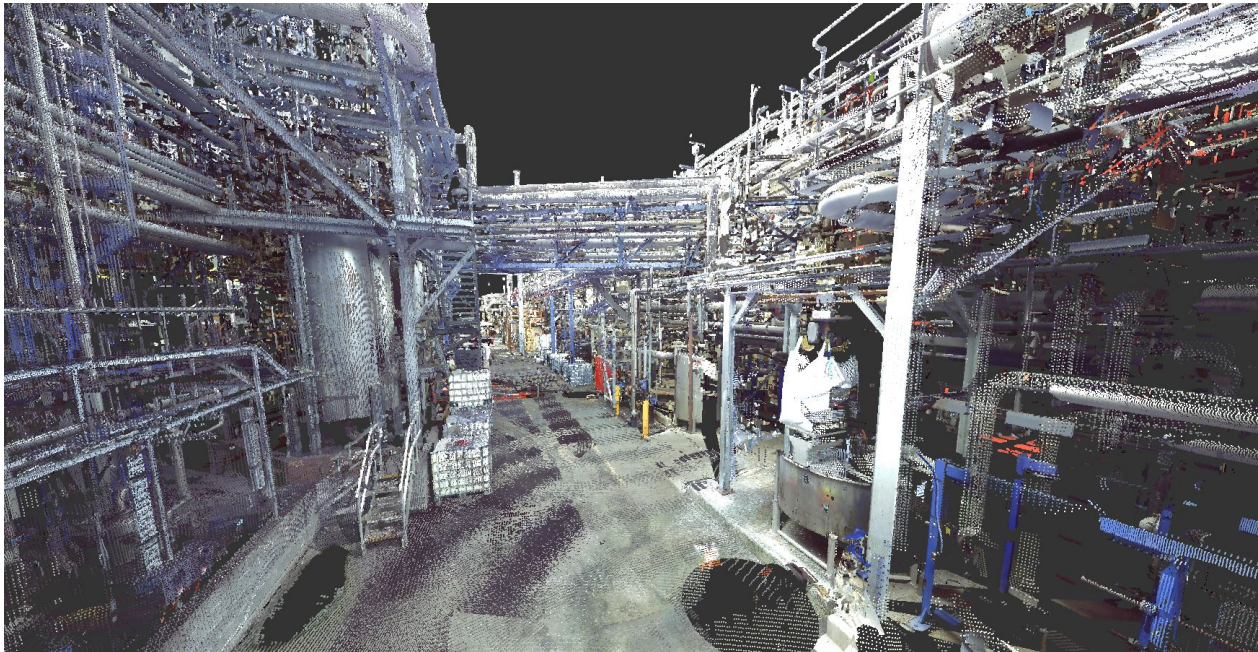
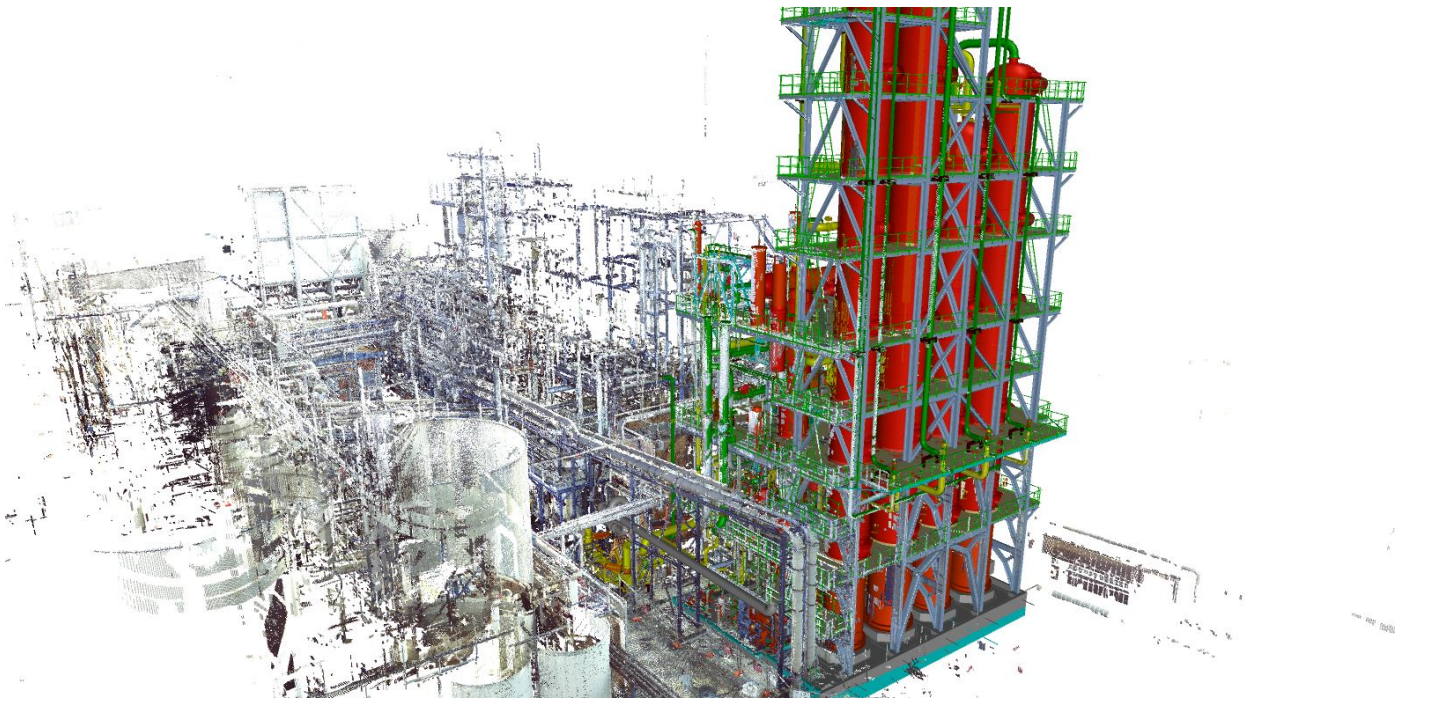


3D scanning

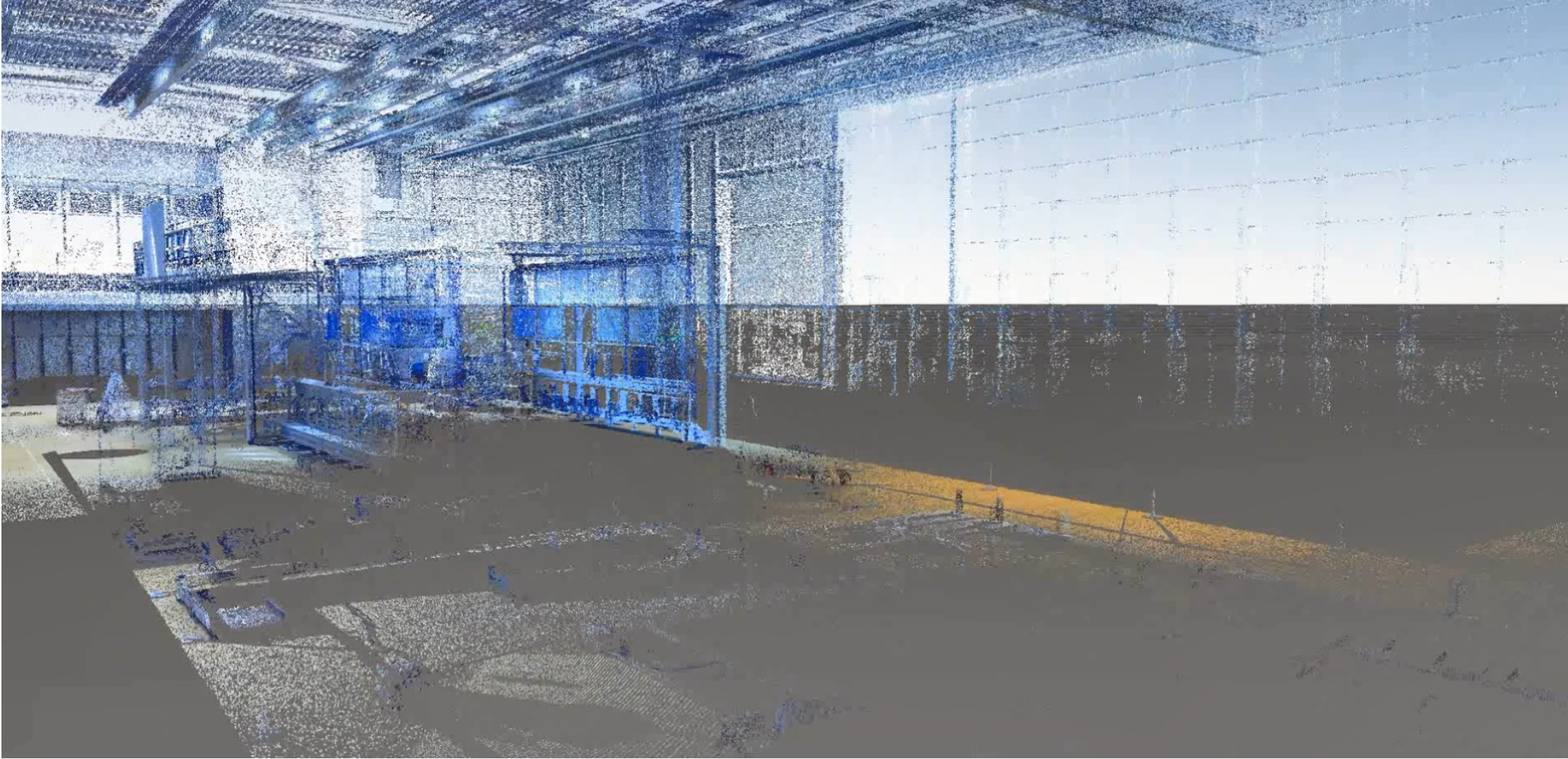
- Plant expansion & modification
- As-designed vs as-built



**WHAT YOU SEE
IS WHAT YOU GET**
advanced 3D scanning & printing



Digital twin - facility



Digital twin – product

Product design

Specification List
05-9111_T [1] - Quality Parameters [Read Only]

Chemical/Physical Parameters

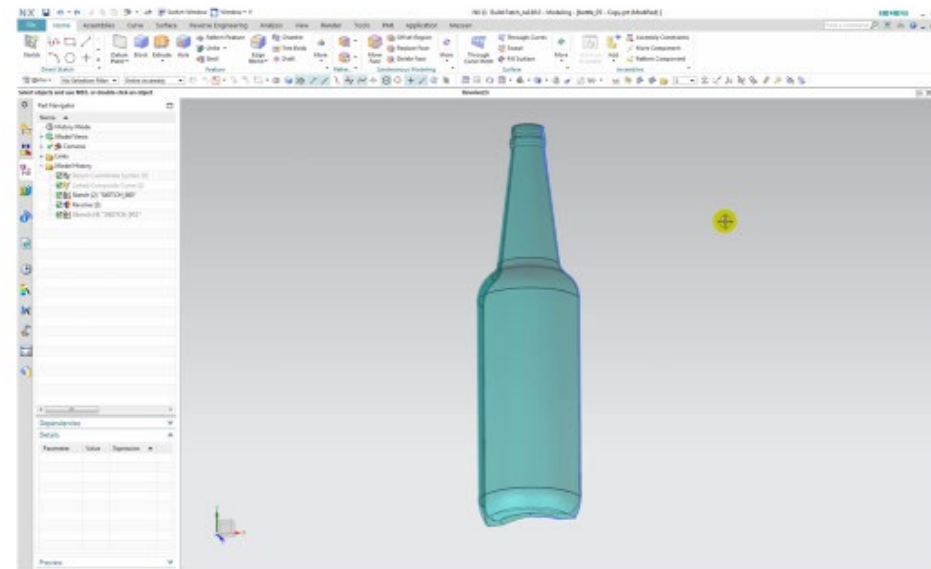
Property	Target	Min Wks	Max Wks	Min Req	Max Req	Unit	Method
pH	4.45	4.35	4.5	4.3	4.6	value	
Foam	250					s	
Colour	8	9	7.5	9.5	EDC	100-2000-47	
Carbon Dioxide	6	7	5.5	6.5	g/l		
Diacetyl	80			100	ppm		
Bitterness	28	31	26	34	IBU		
Apparent Extract	1.8	2.3	1.7	2.5	°Plato		
Apparent Extract - Attenuation Limit	0.4			1.5			
Attenuation Limit	2.2	2.6	2	2.8			

Microbiological Parameters

Property	Target	Min Wks	Max Wks	Min Req	Max Req	Unit	Method
Culture Yeast	0	1		5	value		
Diphtheriae	0	1		5	value		
Killase	0			2	value		
Bacteriocins	0	1		5	value		
lactic Acid Microorganisms	0	1		5	value		
Hydrococcus	0	1		5	value		
Streptococcus	0	1		5	value		
Rod	0	1		5	value		
Water Microorganisms	0	1		5	value		
Wine Yeast	0	1		5	value		

Formulate the product
SIMATIC IT R&D Suite

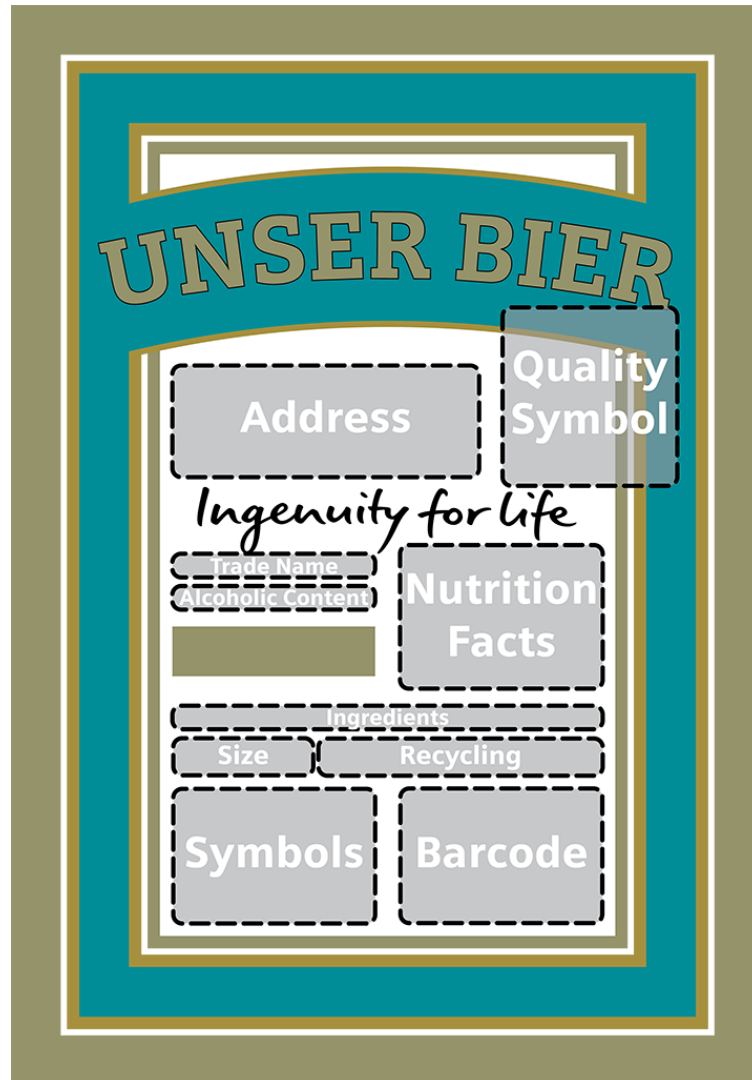
Product design



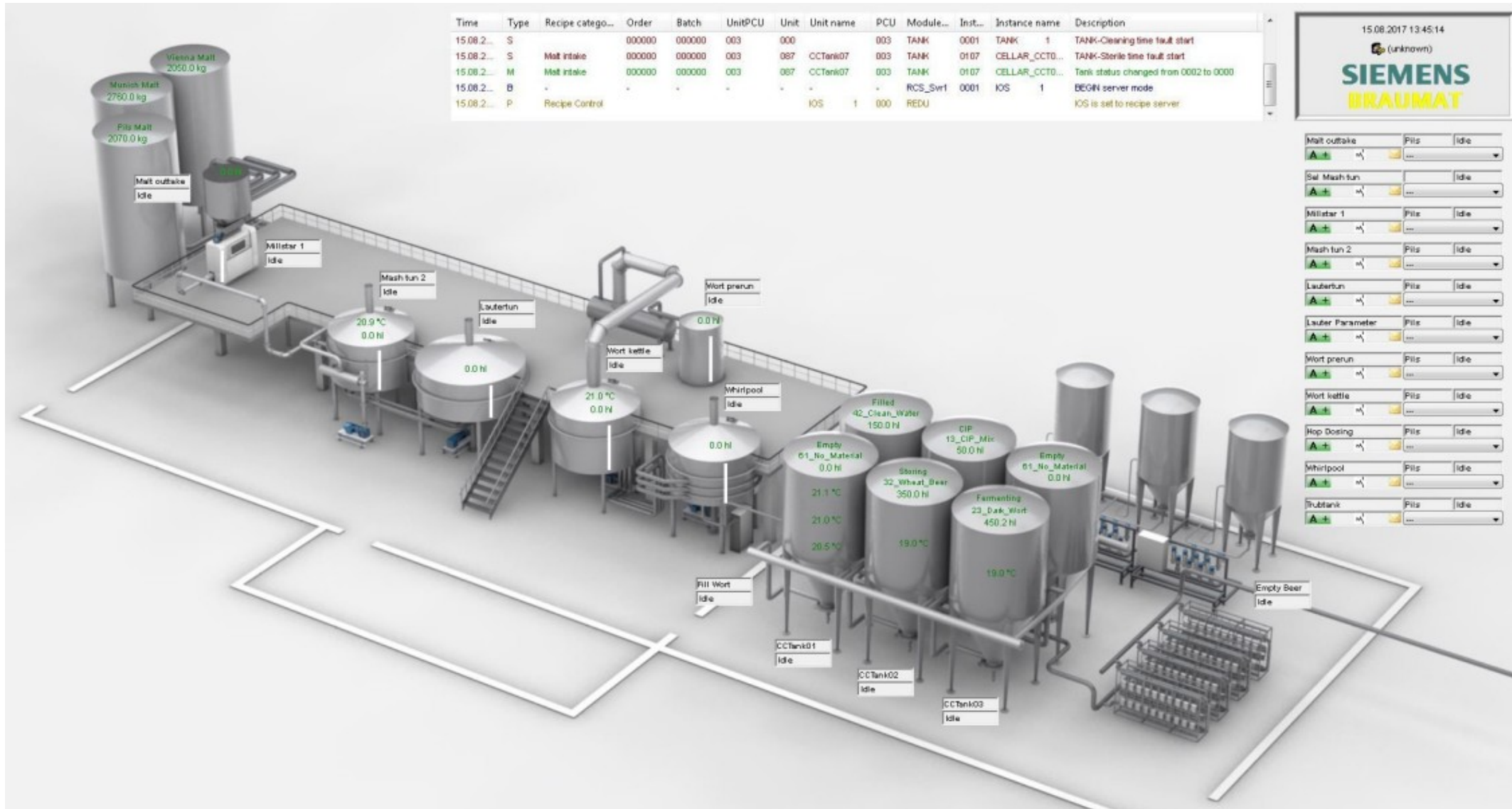
Build the packaging in the virtual world
NX CAD



Digital twin – packaging



Digital twin - process



Industrial IoT

- Craft beer and spirits



DEACAM
FERMECRAFT

Industrial IoT

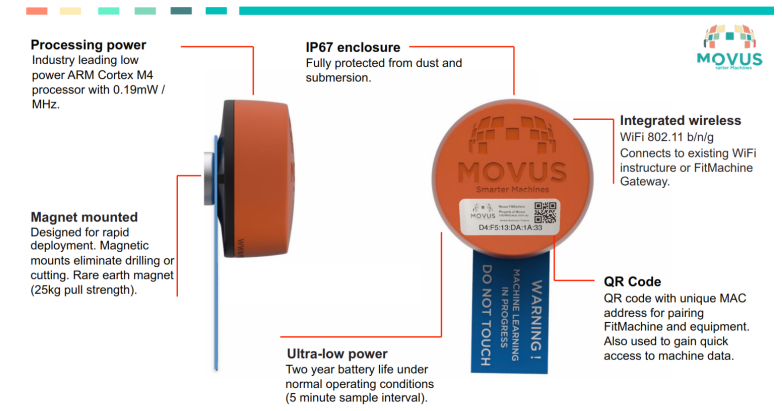


PREDICTIVE MAINTENANCE IS THE WAY FORWARD

The FitMachine® allows continuous 24x7 real time monitoring of industrial equipment, without the need for remote inspections. The FitMachine®, through its machine learning (ML) algorithms that monitor noise, vibration and temperature, can detect when a machine is degrading towards failure and alert maintenance staff to action. Therefore maintenance activities are targeted towards machinery that requires activity, not machines that are working perfectly. The FitMachine® allows a business to drive towards predictive maintenance. This improves staff productivity, safety and equipment availability, while reducing cost.



Early Alerts give you time to plan for maintenance
 FitMachine® PdM Platform helps you cut down maintenance costs
 Remote Monitoring reduces risks and reliability issues



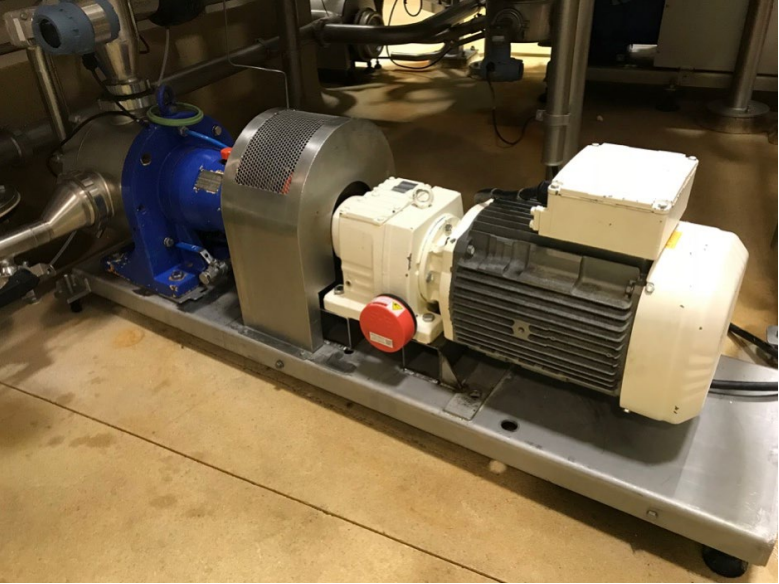
Key features

Wide range of sensing modalities – capture broad environmental conditions	<ul style="list-style-type: none"> Accelerometer Microphone (sound) Barometric Pressure * 	<ul style="list-style-type: none"> Magnetic Field Strength Contact Temperature Humidity *
Low power and ultra long life	4 th generation Texas Instruments (TI) WiFi processor	
Communication	WiFi can operate with existing wireless infrastructure	
Wide operating temperature	Industrial temperature rated electronics for robust long term performance at -40°C to 85°C ambient	
Over the air update	Reprogrammable / customisable over the air (OTA)	

FAST START YOUR INDUSTRY 4.0 TRANSFORMATION WITH A PILOT PROJECT
 GO TO WWW.MOVUS.COM.AU AND SEND US A MESSAGE.



Industrial IoT



Movus

AI Output

Status Site name Sub-area

Overall Condition

06-13 2019

Powered by MOVUS

AI Data Usage All

Measured data

Temperature - Weather

Temperature - Equipment

Zoom 1d 1w 1m All

Equipment usage (%)

From 2017-09-24 To 2017-10-24

Power Usage / day

Equipment Usage / day %

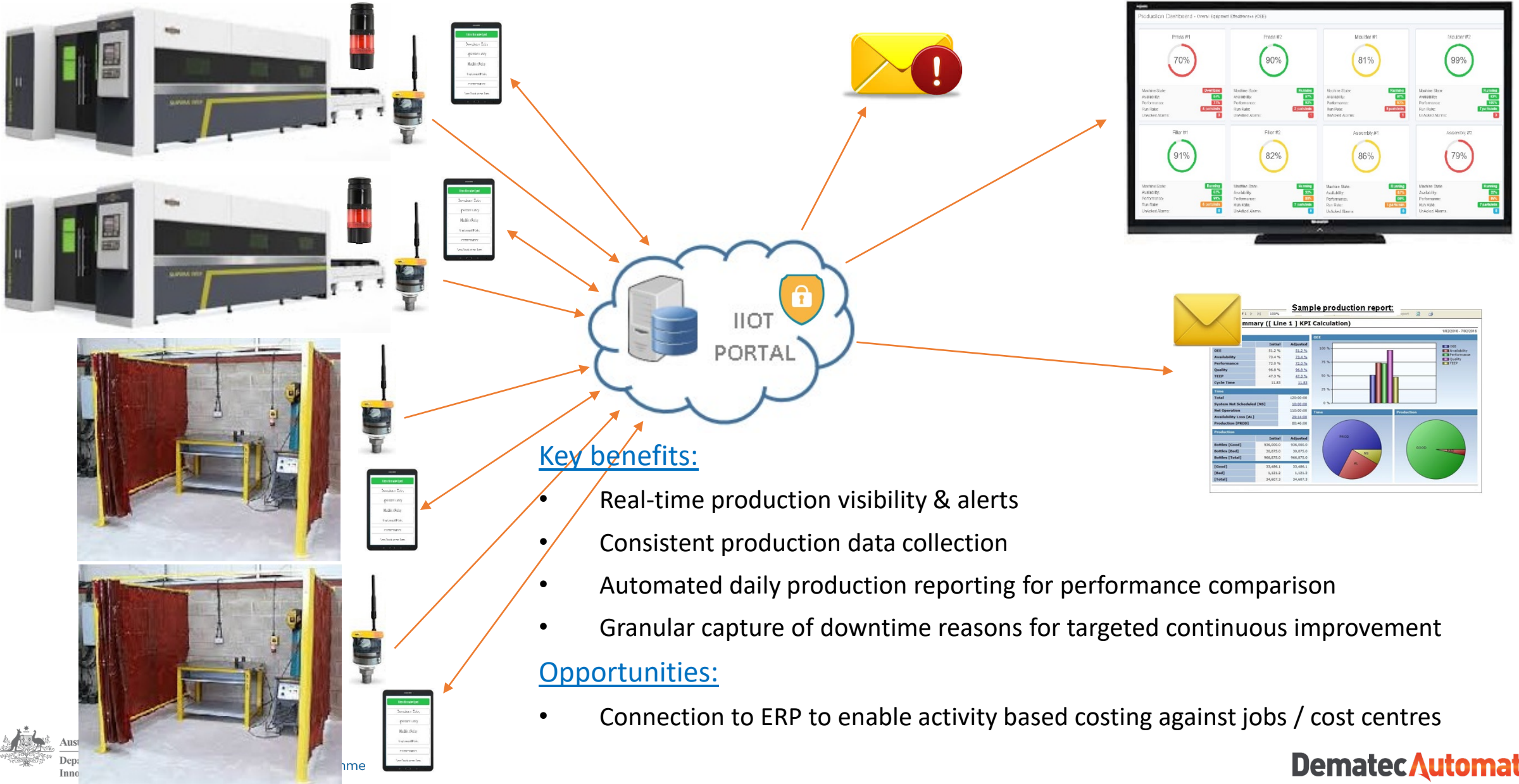
Stopped

Highcharts.com

Equipment Utilisation			
Last day	Last 7 days	Last 4 weeks	Last 365 days
36 %	31 %	56 %	8 %

Estimated power usage			
Last day	Last 7 days	Last 4 weeks	Last 365 days
N/A	N/A	N/A	N/A

IloT - Factory monitoring retrofit

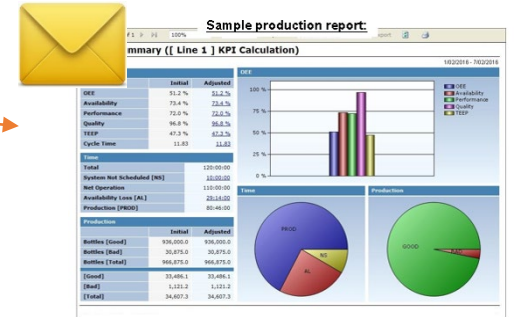


Key benefits:

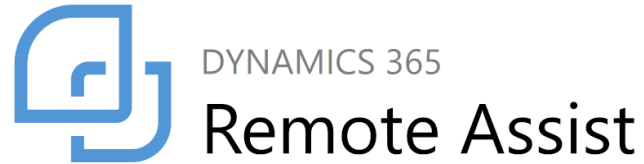
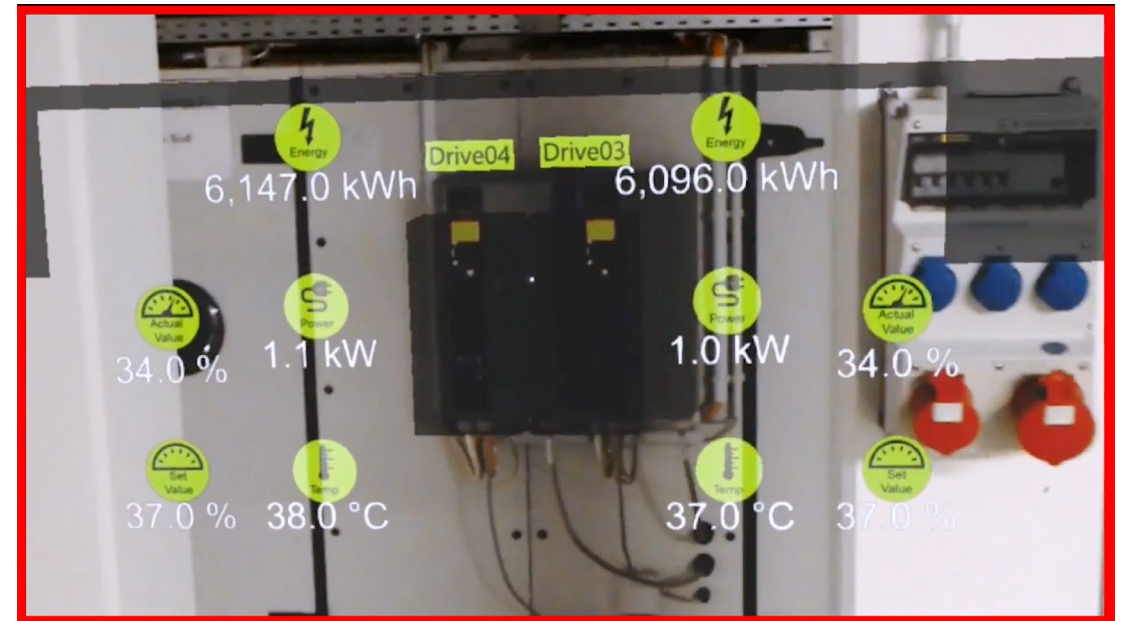
- Real-time production visibility & alerts
- Consistent production data collection
- Automated daily production reporting for performance comparison
- Granular capture of downtime reasons for targeted continuous improvement

Opportunities:

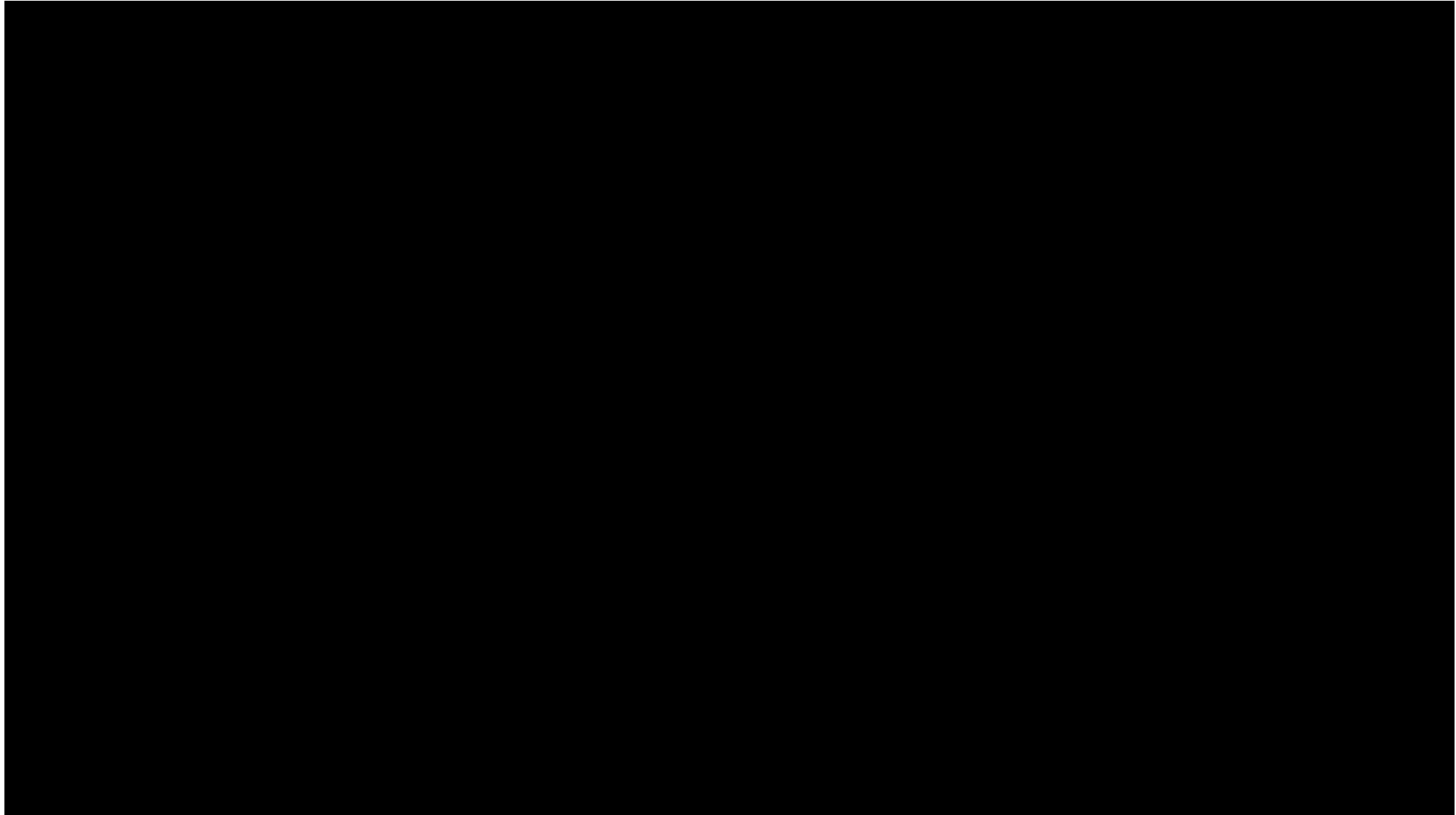
- Connection to ERP to enable activity based costing against jobs / cost centres



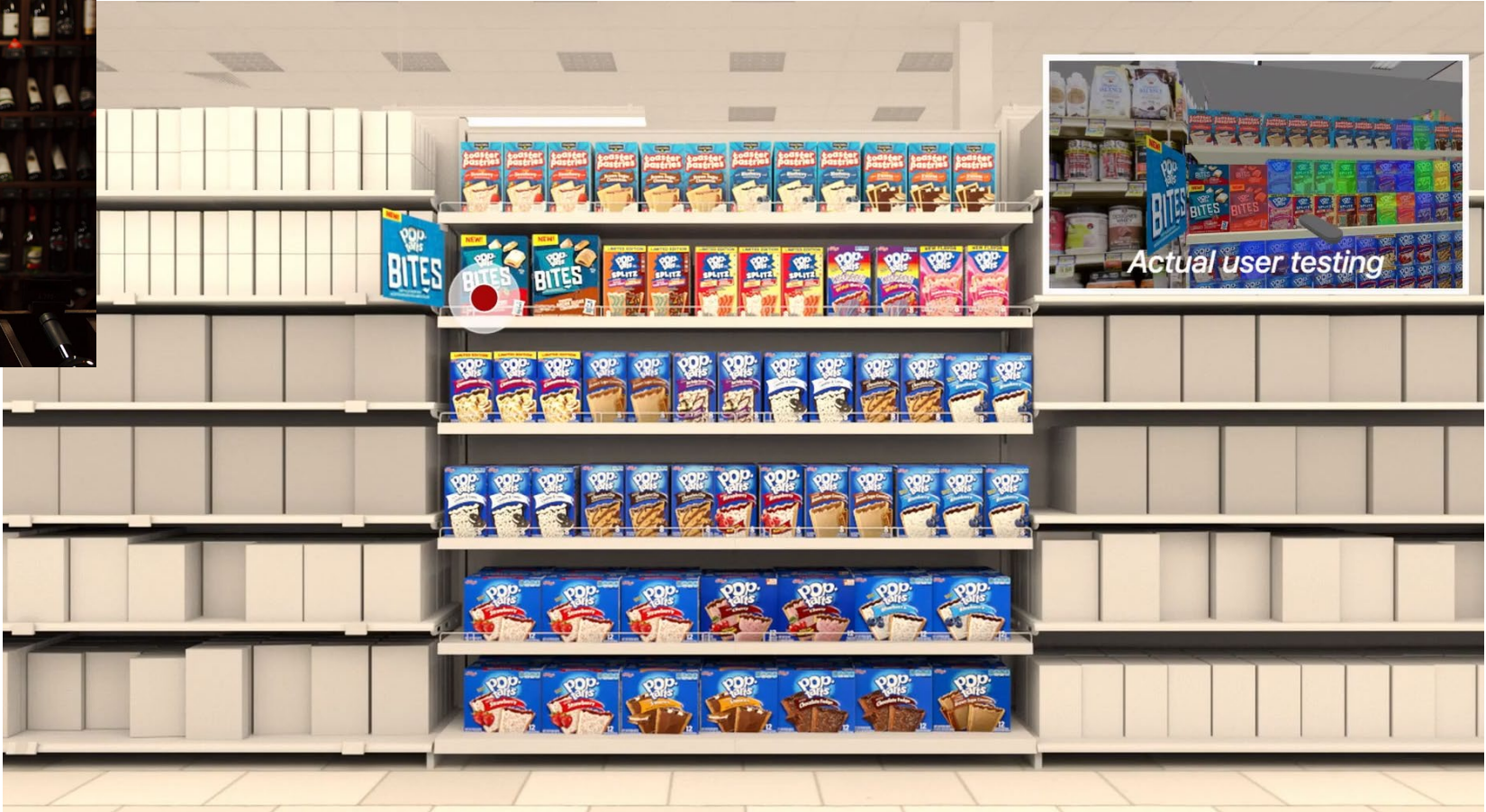
Augmented Reality



Augmented Reality – remote support



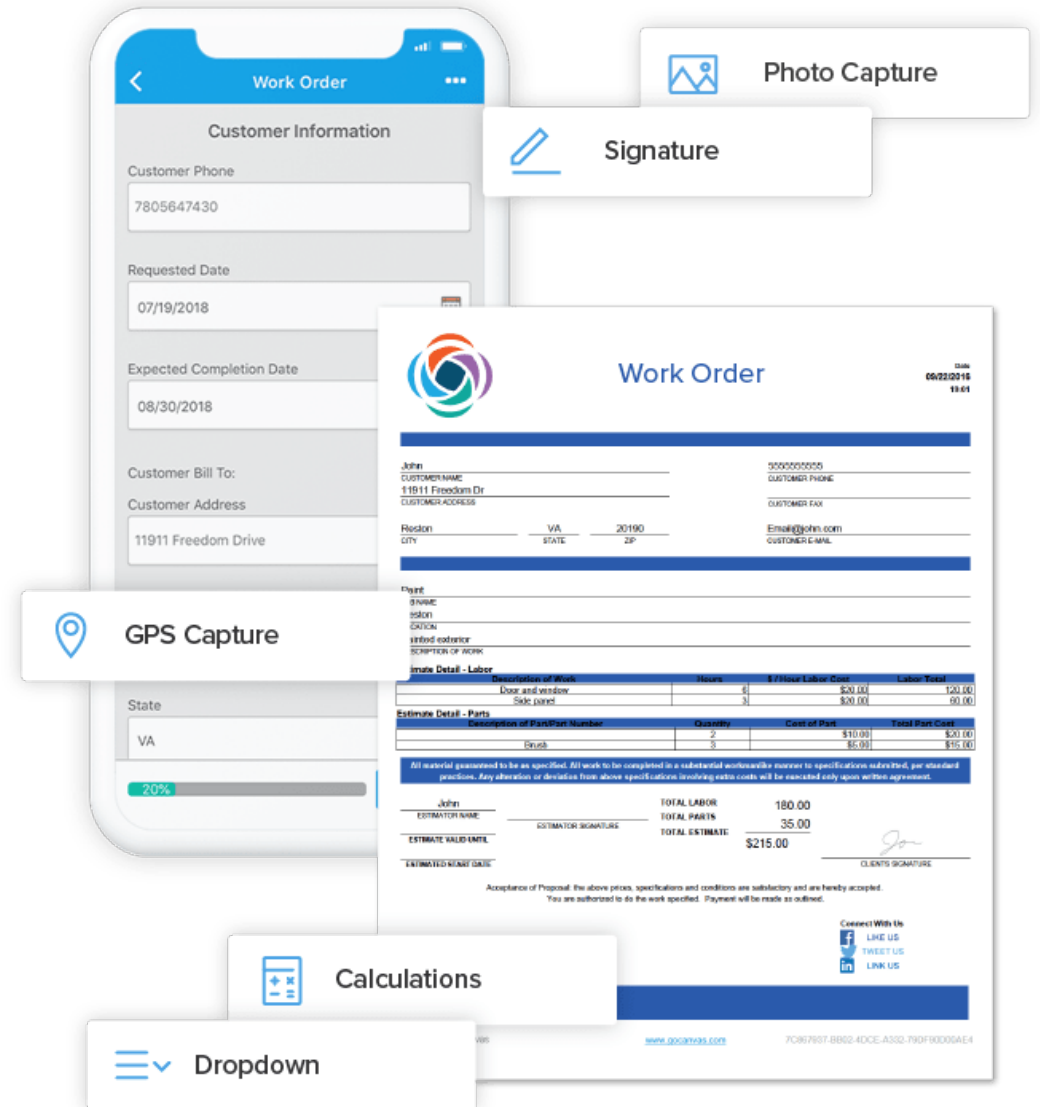
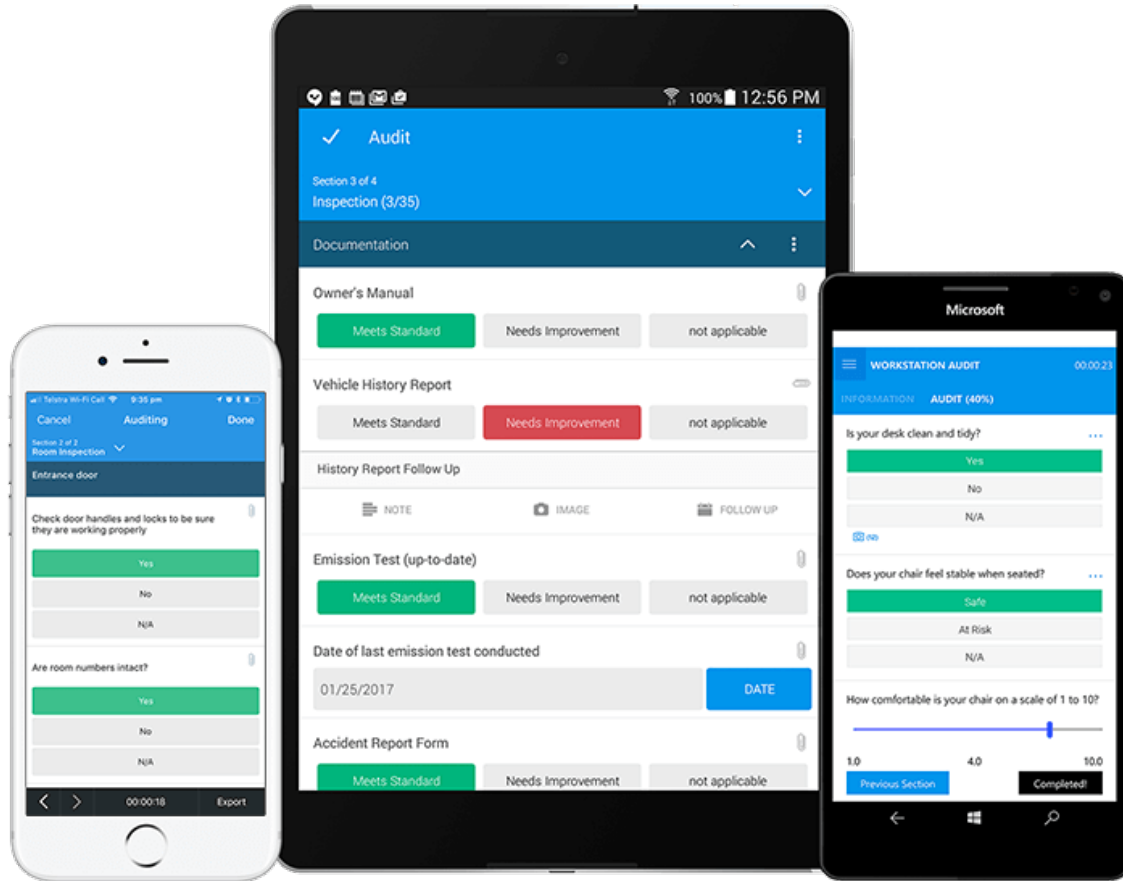
Augmented Reality – consumer testing



Augmented Reality – training



Cloud computing



Cyber Security

THE COST OF CYBERCRIME TO AUSTRALIA

DIRECT COST TO BUSINESS



33% = 693,053 businesses experienced a cybercrime

11,703 reported a cyber incident

153 reports of critical infrastructure



60% OF ALL TARGETED ATTACKS STRUCK SMALL AND MEDIUM BUSINESSES



\$276,323
Average cost of a cyber crime attack to a business

53% of the cost is on detection and recovery

Average cost per attack

Denial of service	\$180,458
Web-based attacks	\$79,380
Malicious insider	\$177,834
Malicious code	\$105,223
Phishing and social engineering	\$23,209
Malware	\$458
Stolen devices	\$13,044
Virus, worm or trojan	\$421
Botnet	\$867

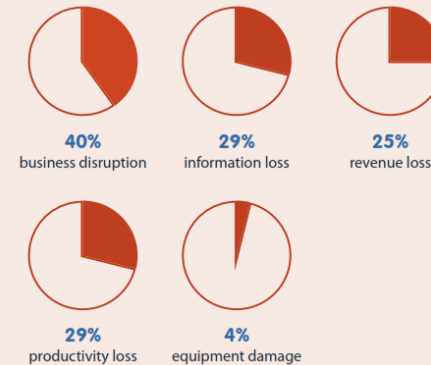
50%

of the costs are caused by web-based attacks and insiders



INDIRECT COST TO BUSINESS

Effect of a cyber attack on business



Average time to resolve an attack is **23 days**



Increase to 51 days if the attack was a malicious insider, employee or contractor.

AT-A-GLANCE

accenturesecurity

NINTH ANNUAL COST OF CYBERCRIME STUDY

Unlocking the value of improved cybersecurity protection

The Ninth Annual Cost of Cybercrime study combines research across 11 countries in 16 industries. We interviewed 2,647 senior leaders from 355 companies and drew on the experience and expertise of Accenture Security to examine the economic impact of cyberattacks.

THE EXPANDING THREAT LANDSCAPE AND NEW BUSINESS INNOVATION IS LEADING TO AN INCREASE IN CYBERATTACKS

Cybercrime is evolving



Security breaches are growing

+11% increase in the last year
130 → 145 Average number of security breaches in 2018
+67% increase in the last 5 years

Technologies introduce risk, and so do humans

79% of business leaders say new business models introduce technology vulnerabilities faster than they can be secured.
Only 16% of CISOs say employees in their organizations are held accountable for cybersecurity today.

ORGANIZATIONS SPEND MORE THAN EVER DEALING WITH THE COSTS AND CONSEQUENCES OF INCREASINGLY SOPHISTICATED ATTACKS

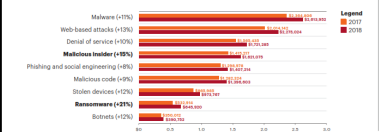
Cost of cybercrime is rising

\$11.7m → \$13.0m +12% = 72% increase in the last 5 years

Business consequences are expensive

\$4.0m Cost of business disruption
\$5.9m Cost of information loss



People-based attacks have increased the most



36% Proportion of reported cost discovering attacks in 2018

© 2019 Accenture. All rights reserved. Accenture, the Accenture logo, Defense and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual authors and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates.

Cyber Security – Information and Services

 Australian Government
 Business
business.gov.au

Cyber Security Risk Self-Assessment Tool

Page 1 of 10

Welcome to the Cyber Security Risk Self-Assessment Tool!

Through a series of questions, this tool will help you understand:

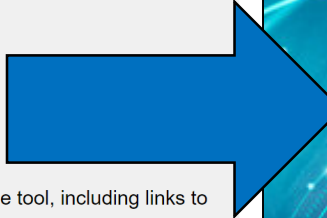
- if your business is a likely target for cyber attacks
- the maturity of your current cyber security practices.


You will receive a tailored cyber assessment report about your business's overall cyber risk on completion of the tool, including links to recommended resources and where applicable, the option to be contacted by our Business Advisers.



The tool will take approximately 20 minutes to complete.

All answers you provide are anonymous - refer to the [business.gov.au privacy statement](#) and [disclaimer](#) for more information.

[Next](#)





 Australian Government
 Business
business.gov.au

Cyber Security Risk Self-Assessment Report

27/06/2018

Results

Overall Cyber Risk Level Rating

High Threat	Yellow	Red	Red
Medium Threat	Green	Yellow with asterisk	Red
Low Threat	Green	Green	Yellow
	High Maturity	Medium Maturity	Low Maturity

Overall Cyber Risk Level Rating Description Low Medium High

OVERALL CYBER RISK LEVEL RATING - how much work your business will need to do to protect your business from cyber security threats.

MEDIUM - Your overall rating indicates that you will need to change some of your practices to better protect your business. The maturity profile of the organisation requires some work in order to better match the current threat profile.

Cyber attacks are a constantly changing threat. Like all risk management activities, you should review your risk profile, internal systems and processes regularly to make sure you protect your business.

THREAT PROFILE - indicates the likelihood of your business experiencing a potential cyber-attack including:

- how susceptible your industry is
- what frameworks are in place
- your business activities.

MATURITY PROFILE - indicates how mature your business is to mitigate the consequences of a cyber-attack, including:

- current IT management
- current security processes.

Next Steps

Business Evaluation

- Find out if you're eligible for cyber security assistance with a [Business Evaluation](#) through the Entrepreneurs' Programme. Business Evaluations provide businesses with access to experienced, independent Business Advisers who review the business, provide an action plan with recommended strategies, up to 12 months of mentoring and up to \$20,000 in matched funding to implement the advice and strategies recommended. Complete the enquiry form above to find out more or speak to an adviser.

Cyber Security Webinars

- Watch our five part Cyber Security [webinar series](#)

Protect your business

- Visit [Stay Smart Online](#) for more advice on how to protect your businesses online. Sign up for cyber security alerts from Stay Smart Online through [Facebook](#), [email](#) or [web](#) for important updates, including news about online threats and vulnerabilities.

Cyber Security Guide

- Download the [Cyber security guide](#) from the Australian Small Business and Family Enterprise Ombudsman website.

Disclaimer: This Cyber Security Risk Self Assessment Report in no way constitutes the provision of professional advice. You should seek independent professional advice prior to relying on material in this report: [business.gov.au/disclaimer](#)

Opportunities for Industry 4.0 technology?

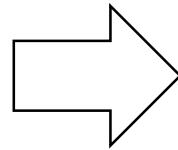
Opportunities in wine engineering?

- Operations management
 - Industrial IoT
 - Remote IoT
 - Virtual and/or Augmented reality
 - Standard Operating Procedures
 - Safety
- Repair and Maintenance
 - Additive manufacturing
 - 3D scanning
 - Real-time condition monitoring
- Plant expansion
 - Process digital twin
 - 3D scanning
 - Industrial IoT
- Product and Process development
 - Product digital twin
 - Process digital twin
- Supply chain
 - Traceability
 - Provenance
 - Quality management
- Resource management
 - Crop monitoring
 - Irrigation / soil quality management
- Marketing
 - Packaging digital twin
 - Consumer engagement
 - Augmented reality
- Remote IoT
 - Irrigation management
 - Crop management
 - Supply chain visibility
 - Personnel safety
- Robotics
 - Crop monitoring
 - Drones

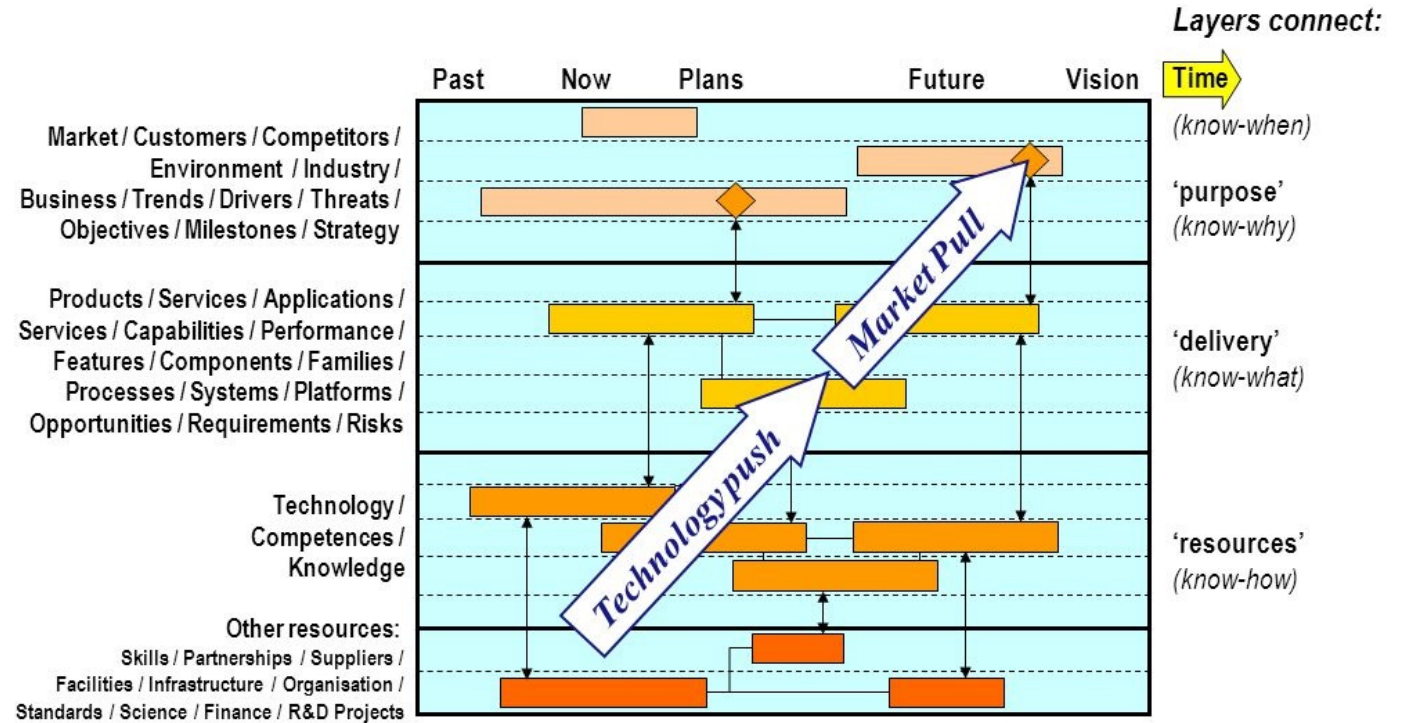
Strategic application

Begins with strategy

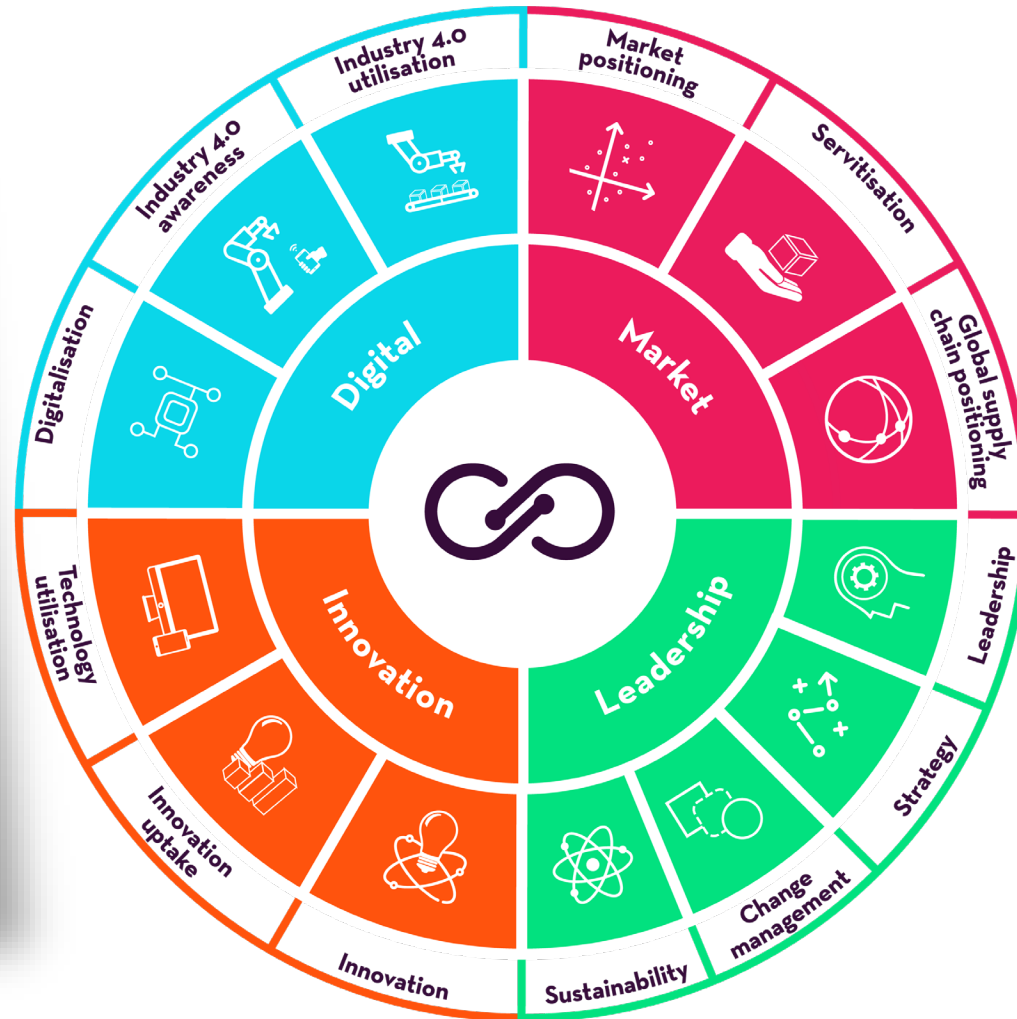
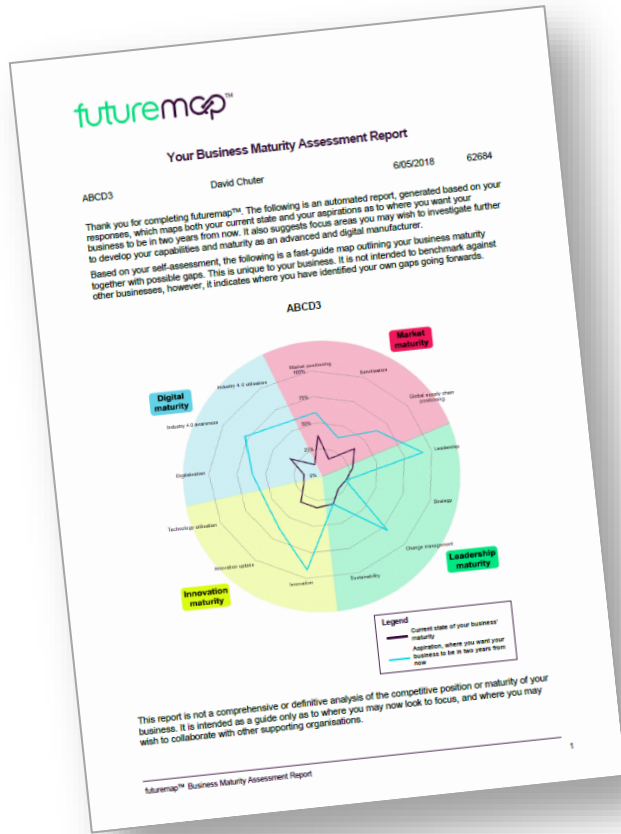
- Business strategy
- Product development strategy
- Marketing strategy
- Engineering strategy
- Technology strategy
- Digital strategy



Technology Roadmap



futuremap™ SME maturity assessment



Getting started

Entrepreneurs' Programme



Australian Government
Department of Industry,
Innovation and Science

SME: \$1.5m - \$100m turnover + 3 years GST registered trading history + solvent + industry growth sector



Business growth advice, facilitation, collaboration

- Guidance, projects
- Matched cash grants
 - Up to \$20K
 - Up to 12 months

Support for industry led R&D with Universities / CSIRO

- Technology guidance, R&D projects
- Matched cash grants
 - Up to \$50K
 - Can be accessed twice
 - Up to 12 months

Support to bring new ideas to market

- Guidance, R&D, projects
- Matched cash grants
 - \$100K up to \$1million
 - 12 -24 months

Support for new and existing incubators

- Guidance, R&D, projects, capital
- Matched cash + in-kind
 - \$26K - \$500K
 - Expert-in-Residence

Entrepreneurs Programme



Australian Government
Department of Industry,
Innovation and Science

- Business Management
 - Business Advisory
 - Technology Advisory
 - bDigital
 - bDesign
 - Supplier Improvement Projects
 - Innovation Connections
 - Research grants $\leq 2 \times \$50,000$
 - Researcher placement grant $\leq 1 \times \$30,000$
 - Accelerating Commercialisation
 - Competitive grant scheme = $\$250,000 \leq \$1,000,000$
- } grants $\leq 2 \times \$20,000$

Thanks and acknowledgements

- Alex Kingsbury – RMIT
- Shane Rolton – WYSIWYG
- David Hart – Dematec
- Brad Parsons - MOVUS
- Leonie Wong – Siemens



Questions?