TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 6-7, 2013

TCIPG OVERVIEW

NOVEMBER 2013

BILL SANDERS AND PETE SAUER

ON BEHALF OF THE ENTIRE TCIPG TEAM

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

WELCOME TO THE TCIPG 2013 INDUSTRY WORKSHOP

- Who is here?
  - TCIPG researchers and students
  - Representatives of industry: utilities, vendors, national labs, ...
  - Our sponsors and external advisory board
- Why have an annual industry workshop?
  - For TCIPG and sponsors:
    - to have impact
    - to communicate our results
    - to get feedback from industry
    - to help choose our research well
  - For industry:
    - to discover and explore TCIPG research
    - to influence future directions
    - to form productive collaborations that can profitably shape the evolving Smart Grid

WELCOME TO THE TCIPG 2013 INDUSTRY WORKSHOP, (CONT.)

- What happens during the Industry Workshop?
  - Sharing TCIPG research results and directions
  - Listening and learning about industry's perspective
  - Stimulating interaction between industry and academics in power and cyber
- Purpose of this talk?
  - Introduce TCIPG – provide context for navigating the next day and a half: who we are, what we do, and why we do it
  - Highlight progress on TCIPG activities
  - Invite your active participation in workshop and in the longer term as well

THE CHALLENGE: PROVIDING TRUSTWORTHY SMART GRID OPERATION IN POSSIBLY HOSTILE ENVIRONMENTS

- Trustworthy
  - A system which does what is supposed to do, and nothing else
  - Availability, security, safety, …
- Hostile Environment
  - Accidental failures
  - Design flaws
  - Malicious attacks
- Cyber Physical
  - Must make the whole system trustworthy, including both physical & cyber components, and their interaction

TCIPG VISION AND RESEARCH FOCUS

Vision: Create technologies which improve the design of a resilient and trustworthy cyber infrastructure for today's and tomorrow's power grid, so that it operates through attacks

Research focus: Resilient and Secure Smart Grid Systems

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications and architectures
- Quantifying security and resilience

PROJECT STRUCTURE

- Site leads coordinate activities at partner schools
  - Dartmouth College (Sean Smith, site lead)
  - University of California Davis (Anna Scaglione, site lead)
  - Washington State University (Carl Hauser, site lead)
- TCIPG stresses industry interaction from inception of research initiatives
  - Pete Sauer, Industry Interaction Lead, co-PI
  - External Advisory Board (9 members) and Industry Interaction Board (more than 300 members)
- TCIPG is organized into clusters of research threads, supporting multiple activities
- Weekly grad-student-led reading group and all-hands meetings

TCIPG STATISTICS

- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009 ($3.8M cost share)
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security, Cybersecurity R&D Center, Office of Science and Technology
- 4 Universities
  - Dartmouth College
  - University of California at Davis
  - University of Illinois at Urbana-Champaign
  - Washington State University
- 23 Faculty, 17 Technical Staff, 38 Graduate Students, 9 Ugrad Students, 2 Admin Staff worked on the project in FY 2013

FY 13 TCIPG SCHOLARLY IMPACT (OCTOBER 2012 – SEPTEMBER 2013)

- Degrees
  - 6 BS/BA, 4 MS, 9 Ph.D.
  - Numerous students at various stages of thesis preparation or defense
  - Graduates have started careers in academia, national labs, and industry
- Publications and Presentations
  - 52 Publications (40 refereed journal/conference,12 thesis/tech rpt.)
  - 144 Presentations in conferences, symposia, industry group meetings, and individual industry partner interaction

TCIPG TECHNICAL CLUSTERS AND THREADS

Trustworthy Technologies for Wide Area Monitoring and Control

- Communication and Data Delivery (5 activities)
- Applications (2 activities)
- Component Technologies (2 activities)

Trustworthy Technologies for Local Area Management, Monitoring, and Control

- Active Demand Management (3 activities)
- Distribution Networks (1 activity)

Responding To and Managing Cyber Events

- Design of Semi-automated Intrusion Detection and Response Techniques (6 activities)

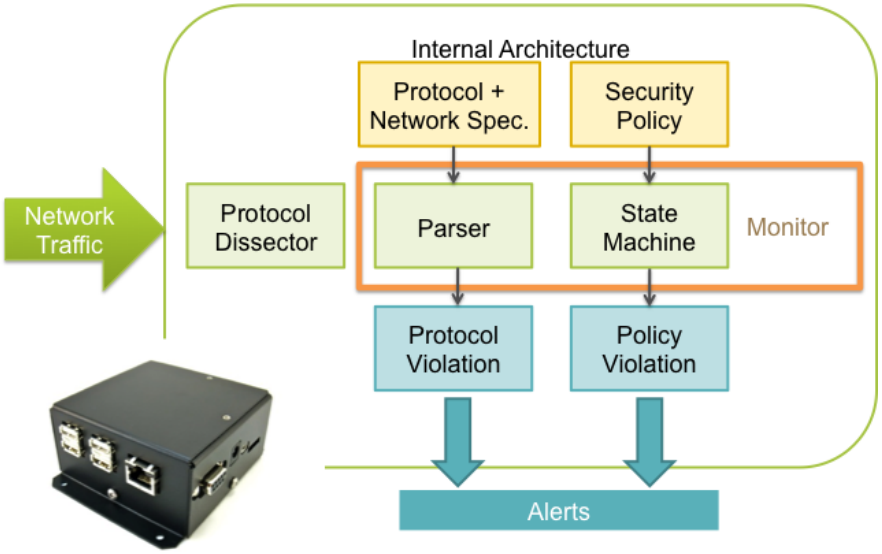
Trust Assessment

- Model-based Assessment (3 activities)
- Experiment-based Assessment (5 activities)

Note: Cluster presentations will be given later in the agenda

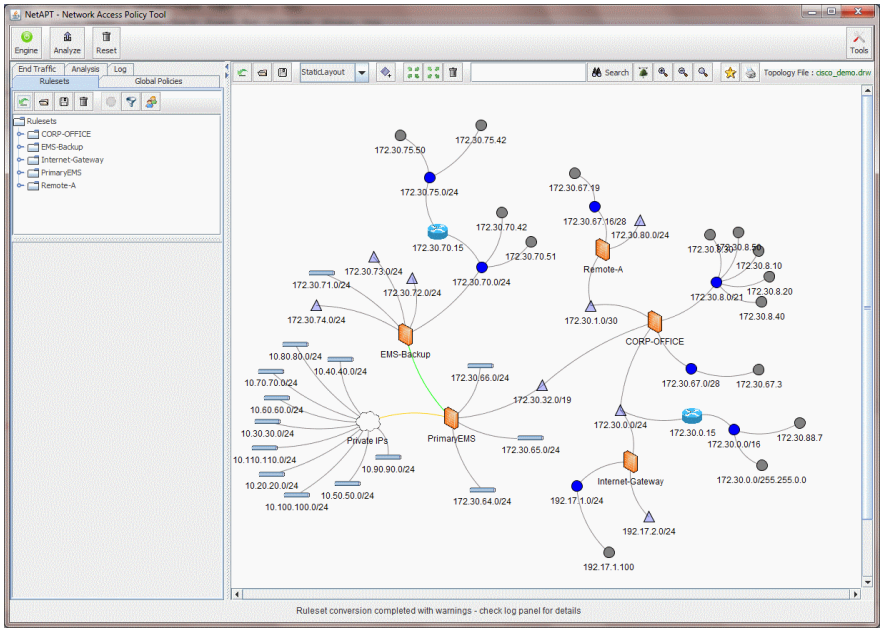
2013 ACCOMPLISHMENTS

- Specification Based IDS for AMI
  - Demonstrated at 2012 Industry Workshop
  - Now in pilot deployment



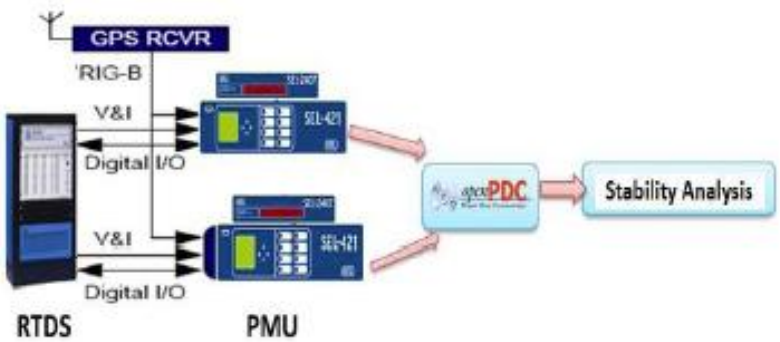
2013 ACCOMPLISHMENTS: NETWORK PERCEPTION

- Based on NetAPT technology developed under TCIPG
  - Static analysis of firewall rulesets
  - Tuned to utility systems, where identifying routable paths to critical cyber assets is an increasingly important problem
- Pilot deployment at major IOUs as technology matured
  - Demonstrated usefulness in NERC CIPS audits
- Used in security assessment of rural electric cooperative utility networks
- Transition of NetAPT from an academic project to a commercial product has been supported at UIUC by a one-year grant from DHS S&T
- Network Perception is now a technology startup

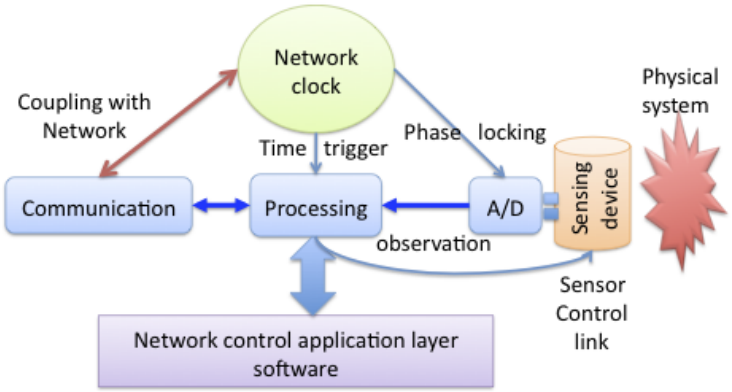


2013 ACCOMPLISHMENTS: ADDRESSING TIME SYNCHRONIZATION CHALLENGES

- Continued study of potential impact of GPS spoofing on wide area measurement systems, and mitigation approaches
- Exploring a time management/sync system that does not rely on GPS
- Developing hardware prototype to evaluate vulnerability and mitigation (Demo)



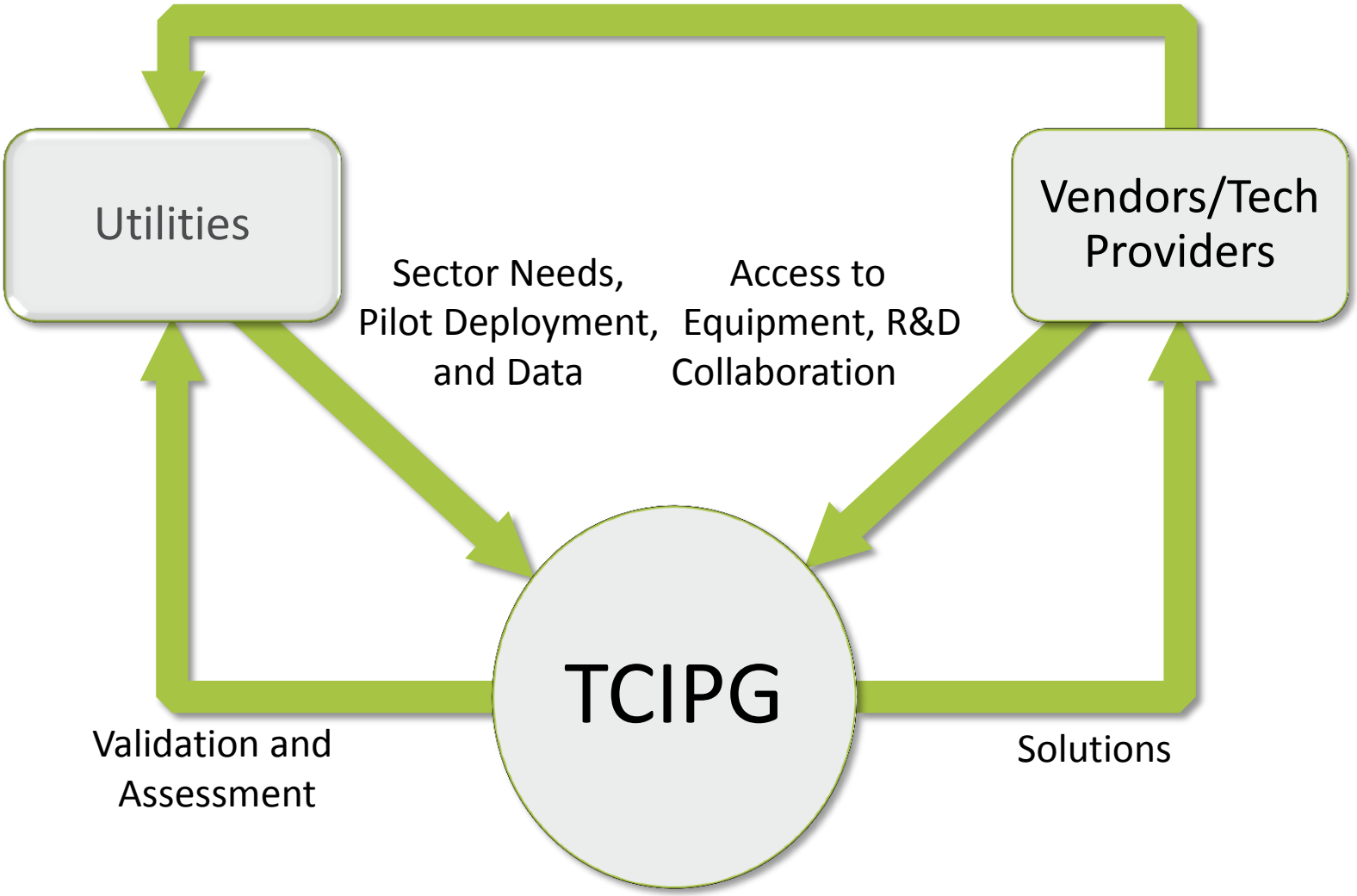
(a) RTDS/PMU/PDC testbed configuration.



TCIPG INDUSTRY INTERACTION

- Engage with Industry early and deeply
- Work on problems where fundamentals can make difference *and* whose solution will be high impact to industry
- Supplement grad student/faculty researchers with professional programmers, power and security engineers to insure “industrial quality” of developed product
- Strategically decide the best method for transfer among: open source, incorporation in existing product, new product, start-up company
- Employ in-house utility expert to help focus research ideas and find appropriate tech transfer targets
- During testing, engage deeply with a small number of users first, and then expand the circle as concept/product develops
- Provide technology transfer support to researchers

TCIPG AS CATALYST FOR ACCELERATING INDUSTRY INNOVATION



COLLABORATION AND TRANSITION

- Utilities
  - AMI Security pilot with First Energy
  - Engagement with EPRI on various fronts
  - NetAPT as NERC CIPS pre-audit tool
  - SIEGate, open communication gateway with Grid Protection Alliance (GPA)
- Industry
  - SEL incorporating TCIPG embedded system security approach in their products
    - Schweitzer is a major donor of TCIPG testbed equipment
  - Honeywell collaboration on Role Based Access Control (RBAC) project in automation systems
  - New industry/academic initiatives with ABB, SEL, EPRI, Honeywell
- National Labs
  - Demonstrated Los Alamos NL quantum cryptography in our testbed, securing PMU communications using a hardware-in-the-loop experiment
  - NetAPT integrated with Idaho NL Sophia security visualization tool
- International
  - “In-Depth Defense of SCADA and Control Systems”, UI and University of Twente (NL), facilitated by DHS S&T and Netherlands Organization for Scientific Research (NWO). In pre-proposal process
- Transition
  - Startups Network Perception and River Loop Security
  - Open source transition of hardware IDS platform and tools for security assessment of wireless networks and SECURE open communication gateway

TCIPG EDUCATION, OUTREACH, AND TRAINING

- Education of professionals versed in cyber and power is the core mission
  - Degree programs
  - Internships
  - TCIPG Reading Group
- K-12 education and outreach
  - Interactive apps and educational kits
    - Over 5K downloads of TeslaTown, over 130K visits to app site
  - Encouraging interest in STEM education and careers
  - Teachers, parents learn too!
- Assisting community colleges in smart grid curriculum development under IGEN Consortium
- Short Courses
- Hands-on security assessment
- TCIPG Summer School
- Annual Industry Workshop

TRAINING: 1.5-DAY SHORT COURSE

- Prepared at the request of our funding agencies (DOE and DHS)
- Geared to program managers
- Topics:
  - Power Grid Equipment
  - Communications and Networking for Utility Computing and Control
  - Basics of Cybersecurity
  - Power Grid Infrastructure Basics
  - Trustworthy Wide Area Monitoring and Situational Awareness
  - Trustworthy Technologies for AMI
  - Cybersecurity Maturity Model

TRAINING: TCIPG SUMMER SCHOOL

- Offered alternate years
- Last session was June 2013
  - Weeklong event, 173 participants
  - Geared to graduate students, utility practitioners, and consultants
  - 20 technical sessions, presented by leading subject matter experts
  - “Deep Dive” on selected topics
  - Hands-on SCADA security assessment training (see next)

TRAINING: HANDS-ON SCADA SECURITY ASSESSMENT

- Six-hour vulnerability assessment exercise of a utility-like system
- Runs on self-contained network
- Established a simplified, “utility-like” virtual environment
  - Included typical security flaws
  - No real systems or actual vulnerabilities
- Students received instruction on
  - Security assessment tools
  - Techniques to analyze public-facing information for security flaws
  - Techniques for mapping networks, exfiltration, and data manipulation
- Very popular at the summer school: added a session by popular demand

TCIPG INDUSTRY INTERACTIONS

Association of Illinois Electric Cooperatives
CLEAN ENERGY TRUST
ENERGETICS
ETRI Electronics and Telecommunications Research Institute
EPRI Electric Power Research Institute
EnergySec National Electric Sector Cybersecurity Organization
FERC
ILLINOIS SCIENCE & TECHNOLOGY COALITION
Illinois VENTURES
IEIA
I3P Institute for Information Infrastructure Protection
NERC North American Electric Reliability Corporation
INL Idaho National Laboratory
OAK RIDGE National Laboratory
Pacific Northwest National Laboratory
Sterne Kessler Goldstein Fox Attorneys at Law
UL
U.S. ARMY
UtiliSec Electric Utility Cyber Security
THINK SMARTGRID

Adventium Enterprises
archimatica
Alcatel-Lucent
ALSTOM
Ameren
at&t
Black & Veatch
BOEING
BT
CISCO
ComEd.
Electric Power Group
DTE Energy
Emerging Threats
ENCARI
Grid Protection Alliance
Entergy
FUJITSU
imagination at work
GENERAL DYNAMICS
GVEA
HARRIS
Honeywell
IBM
Integrated Architecture
intel
Itron
IXIA
JCE
Landis+Gyr
Lockheed Martin
Luminant
McAfee
Mehta Tech Inc.
nationalgrid
n-dimension solutions
NiSource
Northrop Grumman
OSIsoft.
OSI
PATRICK
PG&E
pjm
NIPSCO
QUANTA TECHNOLOGY
SAIC
SEL Schweitzer Engineering Laboratories
SIEMENS
SISCO
PowerWorld Corporation
SPACE•TIME•INSIGHT
Symantec.
Telcordia.
VERACODE
ViaSat
Westar Energy.

LUS Lafayette Utilities System
Los Alamos National Laboratory EST. 1943
neustar
New Hampshire Electric Co-op
PRAIRIE POWER, INC.
S&C ELECTRIC COMPANY Excellence Through Innovation
Raytheon Trusted Computer Solutions
Sandia National Laboratories Exceptional service in the national interest
SHAY LAW GROUP
SRI International R&D for Government and Business
United States Northern Command
U.S.NRC Protecting People and the Environment
VERMONT LAW SCHOOL
westMONROE

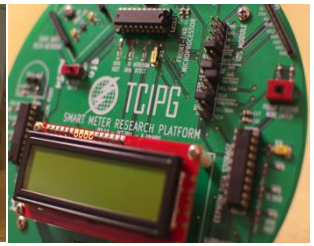
TELEPORT TECHNOLOGIES
Argonne NATIONAL LABORATORY
ASHLAWN ENERGY
ABB Power and productivity for a better world
BAYSHORE NETWORKS
bpa.gov
CORN BELT ENERGY
CAERUS
Eastern Illini Electric Cooperative
epic.org Electronic Privacy Information Center
CYBATI
Exelon
GREEN MOUNTAIN POWER
City of Fulton
Fighting for Illinois Consumers CUB Since 1984
FirstEnergy
Host Integrity Systems
HWS ENERGY PARTNERS
ICS Cybersecurity, Inc.
IOActive™ Using Our Past to Secure Your Future.

TCIPG TESTBED

- A lab-contained but true-to-reality implementation of power grid cyber and physical infrastructure
- Leverages over $6.5 million worth of hardware and software
- Brings together power system equipment, emulation, and simulation
  - Supports cutting-edge research on grid topics from generation to consumption
- Automated for efficient and effective provisioning of power and cyber assets per experiment
- Used for internal TCIPG research, collaboration with national labs, and project with industry

ONGOING TESTBED-CONNECTED INDUSTRY EFFORTS

- ABB
- Applied Communication Sciences
- Electric Power Research Institute
- Entergy
- Grid Protection Alliance
- Honeywell
- Schweitzer Engineering Laboratories
- Many major utilities, coops, and municipalities
- Many national efforts (e.g., NASPI, NIST CSWG, NESCOR, DEFT)



EDUCATION AND ENGAGEMENT, K-12 INITIATIVES

Objectives

- Link researchers, educators, consumers, and students
- Connect with schools and national curriculum endeavors
- Develop interactive lessons and activities and make them available on the web and for touch tablet devices
- Create interest in STEM disciplines and careers
- Illustrate issues necessary for consumer acceptance and use of smart grid technologies

Recent Achievements

- Established a Minecraft private server for hosting a smart grid simulation world
- Planning has begun for a electric grid strategy game for IOS 7 devices
- TCIP Educational materials were showcased at the following events:
  - Project Lead the Way teachers' workshops, July 17 and July 25
  - Panel at IEEE PES GM 2013, "Hands-on Activities for Pre-engineering Outreach"
  - Illinois State Fair Exhibit, August 9 – 18
  - Science at the Market, September 7

SUMMARY

- TCIPG is addressing a complex, multifaceted mission
- TCIPG is a world-leading research center, but uniquely positioned with relationships to industry
  - Identifying and taking on important hard problems
  - Unique balance of long view of grid cyber security, with emphasis on practical solutions
  - Working to get solutions adopted through industry partnerships, startups, and open source
- We are exploring options (beyond end of current DOE/DHS contract) to ensure that we can continue to produce fundamental/high impact results, assist industry, and transfer our developed technologies to industry
- For more information: www.tcipg.org