The Industrial Cyber Physical Security Network (ICPSN)

DRAFT

-: Call to Action :-

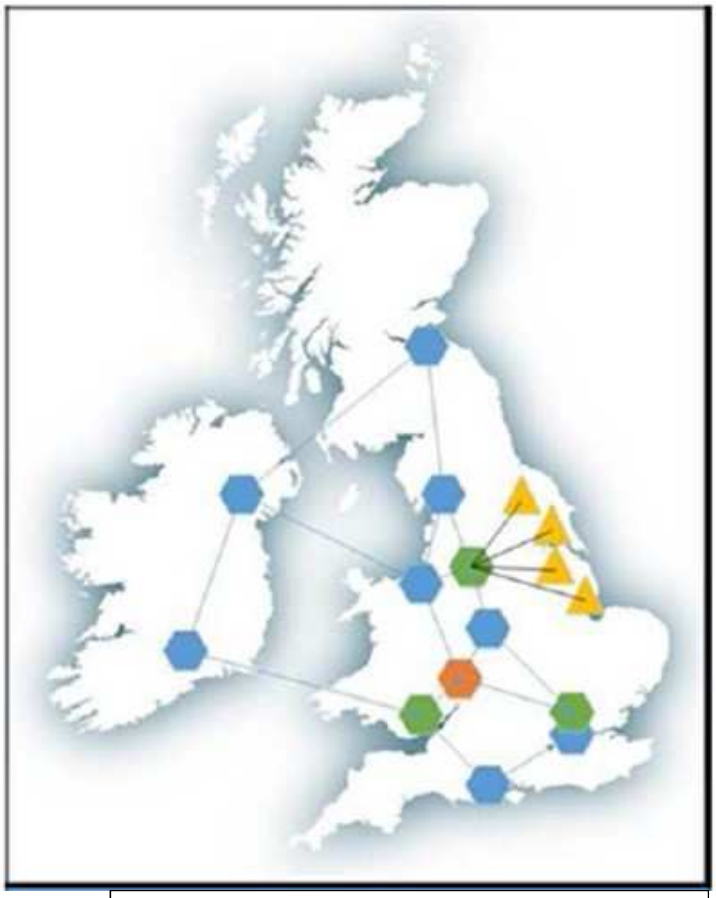
A new independent INDUSTRIAL Cyber Physical Security Network (ICPSN) and Forum is launched.

Across the country for many years there have been groups of like-minded experts and amateurs gathered together to discuss Cyber Threats and potential remedies. Their field and their language have been largely about ***commercial and financial traditional IT*** Cyber Security.

The Industrial Cyber Physical Security Forum is not 'traditional IT', it is Industrial Cyber Physical.

We have mutually beneficial links and exchanges with traditional IT Cyber Security organisations

- Systems Integrators
- Academia
- End-Users
- Vendors
- Insurance
- Agencies
- Institutes
- Global Forums
- Event Providers
- Government
- Institutes
- Individual Experts



Example country ICPSN network nodes

Cevn Vibert
+447909 992786 cevn@vibert.co.uk
Vibert Solutions Ltd. Independent Advice

The ICPSN capability examples: -

- A Secure National Industrial Network between Hub nodes and local organisations.
- Hubs are a mixture of Academia, Integrators, Industry Bodies, Providers and Gov.
- Organisational links with NCSC, UK-CERT, CPNI, Reservists Teams, and many others.
- The Secure ICSN offers users interaction simplified Industrial Red/Blue facilitated events.
- Aid non-Cyber experts to experience real-life events to understand Industrial Cyber.
- Focus on Tier 2, Tier 3 users, integrators, academia and providers but with links to Tier 1.
- A UK go-to system for sharing of resources, help, documents, videos, recordings, etc.
- A semi-secure repository for storing ICS data sets for testing, virus zoo, etc.
- Mobile SOC-in-a-box? ICSN-in-a-pellicase?
- Industrial-Red/Blue-Wargame-Box?
- A network of like-minded people across the UK both ICS and Cyber savvy.
- Shared Industrial NOCs and SOCs – Tiered Holistic Integrated Security
- External links with global organisations such as Webster's ISACS and many others.

… examples of supporting individuals from companies in 2016 ..

Cetix Ltd. , Costain Ltd., Cougar Automation, Elite Control Systems, Kaspersky, L3TRL, Sellafield Ltd., Servelec Controls, Syngenta, Thames Water, Tripwire, Z-Tech Control Systems, Imperial College, De MontFort University, Lancaster University, Birmingham University, QEB University and many more…

Funding and Costs: -

Funding is provided by grants, donations, membership subscriptions and project finders fees. This will be developed as the group grows.

All members will pay an annual subscription to fund both the events, coordination, support services, and the physical and communications network infrastructure management.

Connections to the network will also attract a one-off fee for any security hardware infrastructure and for network setup and support.

The initial aim of the Industrial Cyber Physical Security Network is a non-profit body to support the improvement of the grass roots Industrial Cyber security understanding and collaboration in many countries. This stance and the fees will be continually reviewed for best effect and for sustainability and development.

Cevn Vibert
+447909 992786 cevn@vibert.co.uk
Vibert Solutions Ltd. Independent Advice

-: Call to Action :-

The Industrial Cyber Physical Security Network

Sign-up below.

Company:	
Division:	
Address:	
Postcode:	
Webpage:	
Primary Contact Name:	
Position:	
Email:	
Desk Phone:	
Mobile:	
Contact Name:	
Position:	
Email:	
Desk Phone:	
Mobile:	

I, _____, agree to be invoiced for the 2016-2017 one year membership to support the foundation and forum meetings

Network Node : _____

Forum Membership pa per company : _____

Order Number : _____

You will initially be contacted annually with an invoice from Vibert Solutions Limited. Registered: 10438532 Cevn Vibert, Director

As the Network develops this will change to a formal dedicated organisation with an independent governing body.

Cevn Vibert
+447909 992786 cevn@vibert.co.uk
Vibert Solutions Ltd. Independent Advice

DRAFT

Background:

There is a huge interest in working with real-life systems in both Systems Integrators, Vendors and Academia and many organisations have built their own demo ranges after seeing the range I designed and managed whilst at Thales.

The Network is designed to share resources, methods, applications, developments, procedures and toolsets together with experiences, skills and news.

The need is to fill the current dearth of knowledge and cyber experience across Tier 2 and Tier 3 Systems Integrators, Suppliers and bodies who are not involved in Tier 1 Critical National Infrastructure on a regular basis. These companies have a background interest in current Industrial Cyber news but no regular requirement for Industrial Cyber Delivery from their customers. Both Integrators, and many end-user customers, need education and assisted pathways up the Staircase to Security Improvements.

The UK Government is pushing out Cyber Essentials but this may only address the IT segment who are already best equipped. Best practice directs that Security should be Designed-In to all system solutions. The assistance, experience and environments to be offered by the Industrial Cyber Physical Security Network and Forums will help this situation to improve.

Members will ultimately benefit from attending simple Red/Blue Team Industrial Cyber Physical attack experiences, Cyber Games, links to other suppliers, trainers, consultants and vendors, assistance from mutual beneficial relationships, a sharing of experiences and a flow down of relevant information from Tier 1 and CNI.

The physical network link will provide shared access to other members Cyber Ranges / Industrial Cyber Physical Security Test Beds.

Cevn Vibert
+447909 992786 cevn@vibert.co.uk
Vibert Solutions Ltd. Independent Advice