Products/Solutions/Expertise of C-DAC Mumbai in Smart City Domain

SCADA Security Products

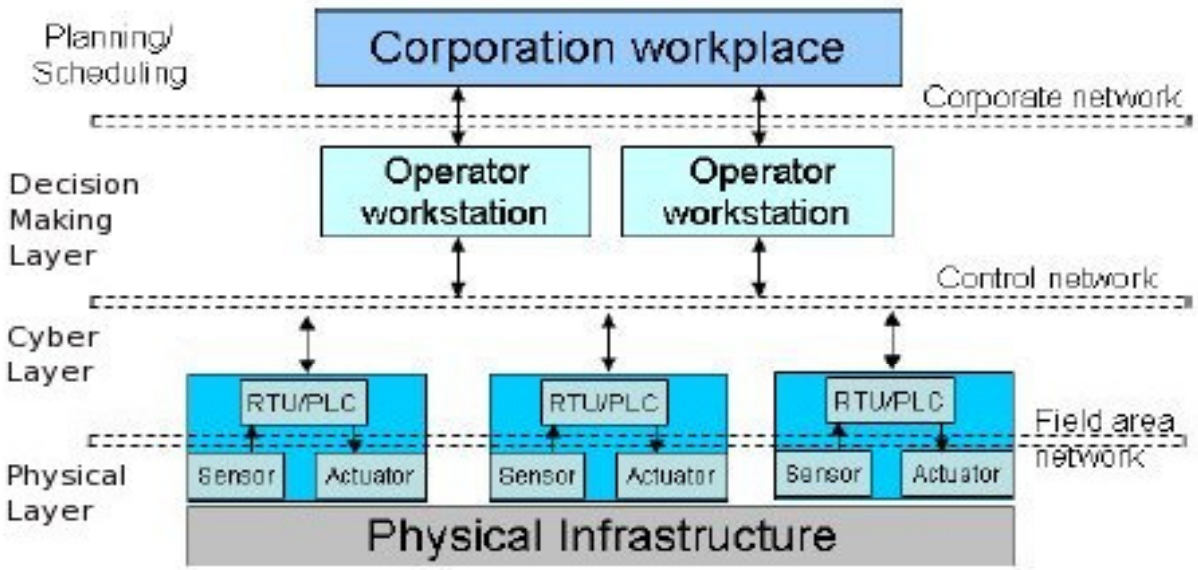
28th February 2017

CDAC Mumbai

SCADA Security Products

Sr. No.	Product Name	Category	Features	Suitable user agencies / customers	Hardware & Software Requirements
1.	Bump in the Wire (BiTW) Device	Industrial control communication system security	It can Secure the communication between RTU and MTU using SecKey-D (CDAC's Patient pending) protocol & Flexi-DNPSec Protocol	ı Power Grid (Electric Substations) ı Power Generating Stations ı Distribution Agencies	ı ARM Board ı Serial RS-232 Port
2.	Vajram Tool	Industrial control system security	It can detect malicious polled response from the grid and the command manipulation	ı Power Grid (Electric Substations) ı Power Generation Stations	ı Octave ı Psat ı Linux ı GTK ı 2 GiB RAM ı 20 GiB H/D ı 64 bit architecture

SCADA Architecture



Need of CDAC Products

SCADA Vulnerabilities:

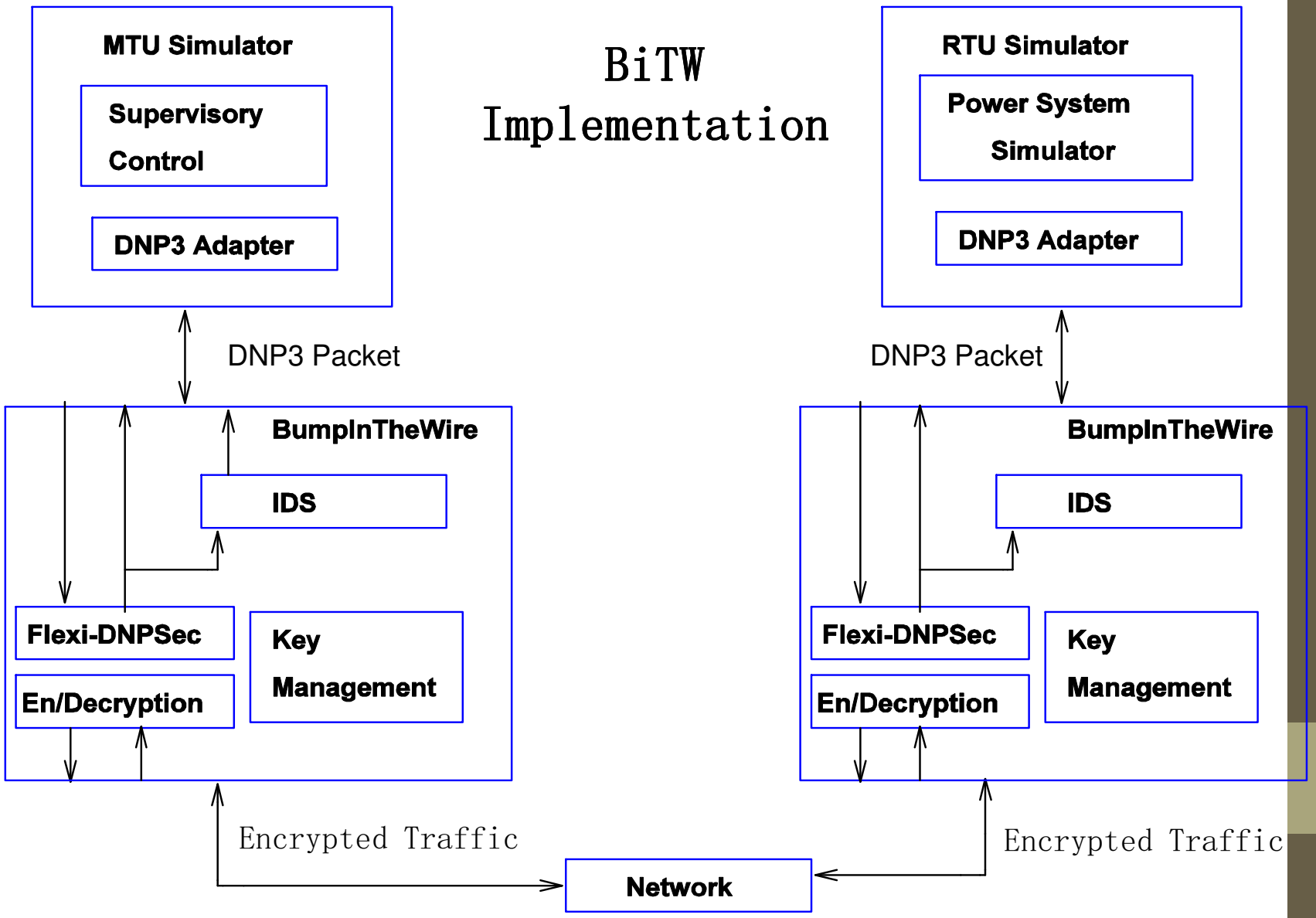
- Architectural vulnerabilities
- Security Policy vulnerabilities
- Software vulnerabilities
- Communication Protocol vulnerabilities
  - Distributed Network Protocol ver 3 - DNP3
    - Lack of mechanisms for authentication, authorization and encryption
    - Headers at different layers of the protocol can be manipulated for intrusions

Need of CDAC Products

Cyber-Attack Incidents:

- March 1997: Worcester Air Traffic Communications Attack
- January 2000: Maroochy Shire Sewage Spill
- 2000 and 1982: Gas Pipelines in Russia/Soviet Union
- January 2003: Davis-Besse Ohio Nuclear Power Plant and the Slammer Worm
- August 2003: Northeast Power Blackout
- August 2005: Automobile plants and the Zotob Worm
- July 2010: Stuxnet attack at Iranian nuclear power plant
- July 2012: Northern grid failure in India (we can't deny such a possibility)

SCADA Security Architecture



Need for SCADA Simulator (Vajram)

- Testing of developed security solutions directly on real power system is not feasible
- Bridges the Cyber-Physical divide by bringing in the Physical system inside the Cyber domain
- A grid is too complex to be set up with analog scaled down models
- Test environment using bulk power system components and control software is costly

SCADA Simulator

- Systems View
  - Grid elements (bus, line, generators, loads, transformers)
    - Power System and Analysis Tool (PSAT) can simulate electrical grid
    - Takes a Matlab/Octave file as input
    - It consist of initial configuration of grid elements constituting the system
    - This is used for power flow analysis of the system under purview
    - Outputs power-flow results for buses and lines

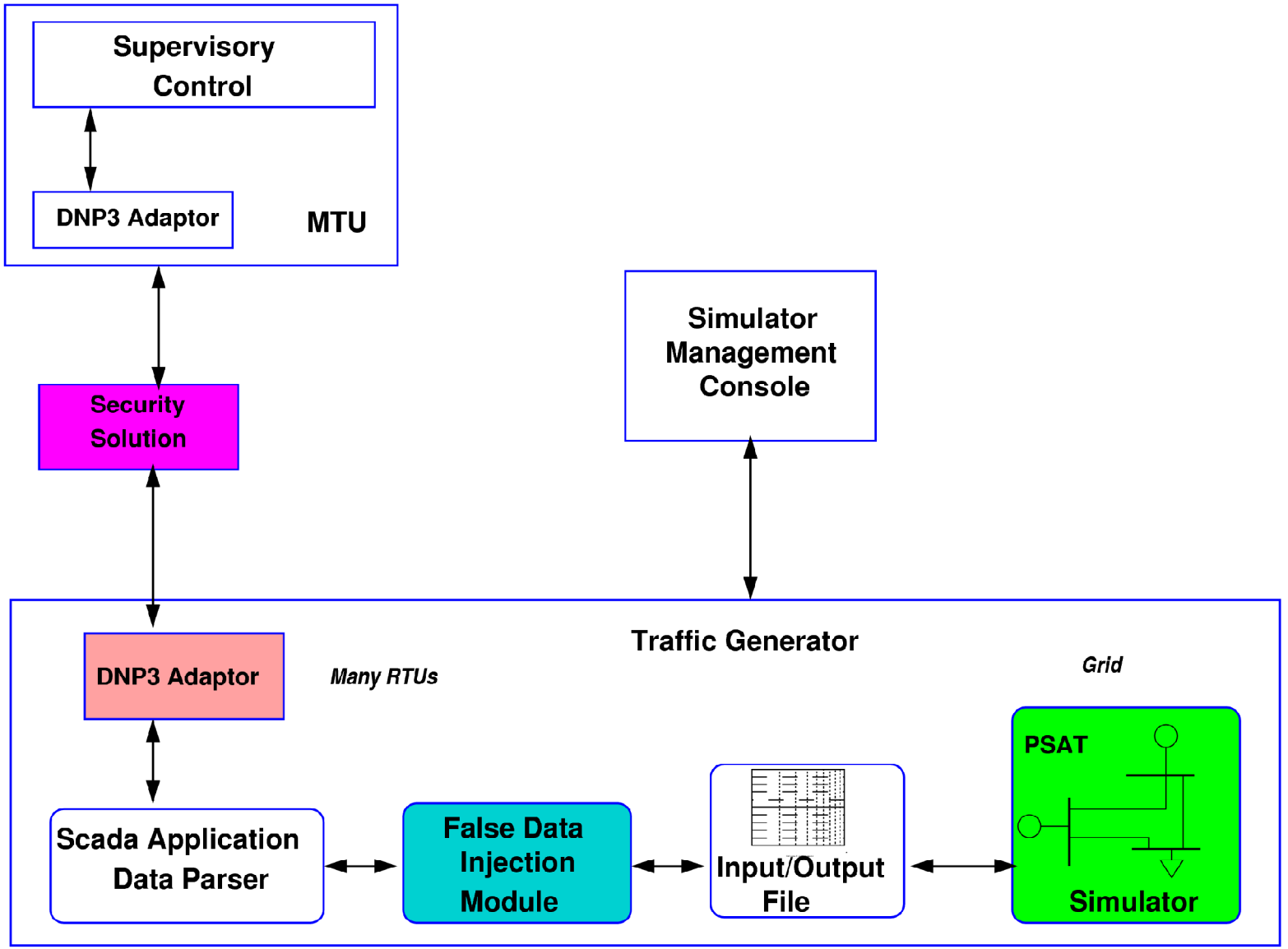
SCADA Simulator

- SCADA View
  - MTU, RTUs, Sensors
    - Grid is populated by multiple RTUs
    - Each RTU is connected to a number of grid elements
    - Grid elements are defined as structures
    - The RTU conveys commands to grid elements
    - RTU also transfers the data from grid elements to MTU
  - Communication Protocol
    - Protocol adaptor
    - Mapping of packet elements to respective grid elements

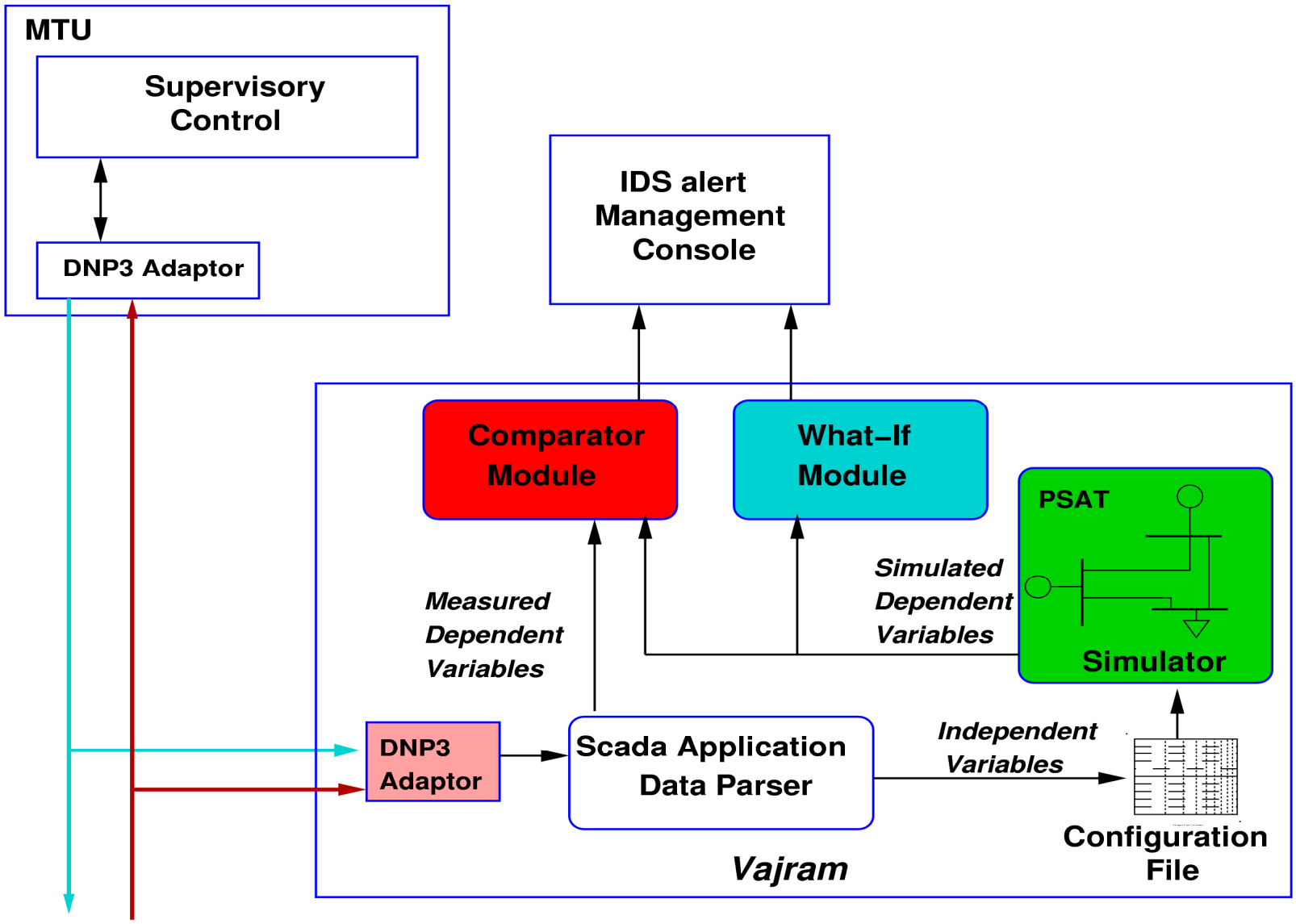
Uses of Vajram

- Three uses of Power System simulator
  - Traffic generator
  - Comparator
  - What-if analysis
- The security solution with Comparator and What-If modules is named as 'Vajram'

Traffic Generator



Vajram


MTU
Supervisory Control
DNP3 Adaptor
IDS alert Management Console
Comparator Module
What–If Module
PSAT
Simulator
Simulated Dependent Variables
Measured Dependent Variables
DNP3 Adaptor
Scada Application Data Parser
Independent Variables
Configuration File
Vajram

Thank You

www.cdac.in

प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
Gulmohar Cross Road No. 9, Juhu, Mumbai - 400 049
Maharashtra (India).
Phone: +91-22-26201606/1574 Fax: +91-22-26232195/ 26210139