FMEA									
Scope and Boundries									
The electrical grid system consists of human-machine interfaces (HMIs), servers (SVs), energy boxes (EBs), intelligent electronic devices (IEDs) and Ethernet links. Including measurement units, protective relays and controllers, IEDs serving as interface devices between power and communication network. Each IED shall track, regulate and optimize the effective use of energy between generation and load. The commands received from HMIs also apply. Metering Infrastructures, such as EBs, are connected to electrical grid stabilizer systems to collect data on the energy usage of electricity grid stabilizer systems between various IED controllers and their respective power elements. Please note that each consumer is believed to be connected to one EB and, in the model, a general EB represents all related EBs. Through IED or EB is connected to a SW via an Ethernet communication which redirects data via the corresponding communication links. TA key SW gathers information and sends it to the corporate and control center from all points of the network.									
Compent	Functionality	Failure Mode(s)	Failure Cause(s)	SEVERITY (1 - 10)	Failure Effect	OCCURRENCE (1 - 10)	Detection method	DETECTION (1 - 10)	RPN
Human-Machine Interface (HMI)	Primary tool by which operators coordinate and control the grid	Power outage	Remote disconnection of power	8	HMI disconnection from the communication network; impossibility to monitor and/or control the grid in real-time by manual operation. No system monitoring; corrective and/or preventive manual commands are not properly executed, or can't even be impossible to execute.	2	Loss of power; HMI blackout	1	16
		Operational failure	Poor communication between HMI and other cyber components	6	Impossibility to monitor and/or control the grid in real-time via manual operation; wrong control commands. No system monitoring; corrective and/or preventive manual commands are not properly executed, or can't even be impossible to execute.	6	Real-time monitoring	6	216
			Human error	5		8	-	6	240
			Poor software design	6		7	Software malfunctions detection; inability to execute manual actions	6	252
		Security failure	Direct human intrusion: faulty commands (cyberattacks)	6	Loss of integrity. Ennergy systems applications run under inadvertent commands; inadvertent operations in the power system, which can lead to partial losses of energy; possible blackout.	4	Erroneous/illogical commands made without operator's consent; firewall block; attempt to pass the firewall	8	192
			Human Vengeance	6		3	-	8	144
Server (SV)	Computing system platform used for various network communication applications / computer program or device that provides functionality for other programs or devices	Data overload	Lower storage capacity or unexpected large amount of data to storage	4	Large amount of data is lost; defective storage of data. Energy system applications are compromised.	4	SV has low data storage capacity	2	32
		Hardware crash	Overheating and high humidity	6	Impossibility to access system's information. IT malfunction; Energy system applications fail or are compromised.	4	Temperature monitoring	1	24
			Hard drive crash			4	SV blackout	1	0
			Hardware sabotage			2	Physical surveillance	1	0
			Physical disaster (such as fire, earthquake, lightning or flooding)			3	Weather monitoring	1	0
		Data errors	Software malfunction	5	Impossibility to access system's information. IT malfunction; Eergy managemetn applications fail or are compromised	5	Unexpected behaviour	3	75
		power outage	Remote disconnection of power	6	Impossibility to access system's information. Energy systems applications fail or are compromised	3	Loss of power	1	18
		Security failure	Denial of service attack (DoS)	5	Loss of data integrity; deleted or corrupted data. Energy systems applications run under fallacious information; inadvertent operations in the power system; loss of integrity	5	Firewall block; attempt to pass the firewall; suspicious system behaviour	3	75
			Hacking for sensitive information	6		5	Firewall block; attempt to pass the firewall; suspicious system behaviour	8	240
			Malicious software infection	6		5	Firewall block; attempt to pass the firewall; suspicious system behaviour	8	240

Network link	Physical component responsible for assuring a message is sent from one network node to another node (local distances)	Cross talk (overload)	Excessive traffic/ congestion of packets	4	Delays in data communication; corrupted signal. Deterioration of communication network performance; Deterioration of communication network performance; energy system applications are compromised	3	Deterioration in communication network performance	5	60
		Network link integrity defect	Manufacturing imperfection	5	Delays in data communication; no data transmission. Energy system applications are compromised (non-optimal asset management); decrease in communication network performance	4	Electrical test and quality assessment	5	100
			RJ45 degradation	5		3	Visual inspection	5	75
			Incorrect installation	5		4	nspection after installation	5	100
		Network link breakdown	External damage (accidents)	5	Cable break; loss of communication between cyber-equipment. applications are compromised (non-optimal asset management); decrease in communication network performance	5	No communication	5	125
Energy Box (EB)	Electronic device used to record and communicate electric energy consumption for monitoring and controlling purposes	Communication Error	Poor signal with SV	2	Defective or even no transmission of data. energy system applications run under lack of information (non-optimal asset management); inadvertent operations in the power system	4	Inability to get EB reading	4	32
		Power consumption misreading	Manual manipulation	8	Incorrect data acquisition. applications run under lack of information (non-optimal asset management); loss of efficiency; loss of power quality	4	Record of abrupt drop in power supply; comparison between registered and expected load diagrams	6	192
			Significant measurement error, or even inability to measure power consumption	8		4	Comparison between registered and expected load diagrams	4	128
		Operation failure	Improper EB programming and parameterization	7	Incorrect data acquisition, or even no data acquisition. Energy system applications run under lack of information (non-optimal asset management); inadvertent operations in the power system	5	Comparison between registered and expected load diagrams	5	175
			Erroneous installation	7	Incorrect data acquisition, or even no data acquisition. Energy system applications run under lack of information (non-optimal asset management); inadvertent operations in the power system	5	EB test and quality assessment	4	140
			Power supply failure	7	No data acquisition. Energy system applications run under lack of information (non-optimal asset management); inadvertent operations in the power system	5	-	2	70
		'Catastrophic' failure (burning, melting or explosion)	Temperature stress	9	Degradation of surrounding smart meter components; personnel injuries or death. Energy system Degradation of surrounding smart meter components; personnel injuries or death	3	Temperature monitoring	1	27
		Security failure	Hacking for personnel sensitive information or faulty information injection (cyberattack)	7	Loss of data integrity. Energy management applications are based on fallacious information	5	Detection method	8	280
		Communication	Damaged transducers	6	Incorrect data processing due to erroneous or incomplete data acquisition; inadequate processing of data; inability to communicate with control center unit. Corrupted communications; Energy systems applications fail or are compromised (non-optimal asset management); decrease in communication network performance.	4	Inability to establish communication with IED	3	72
			Poor communication between IED and remaining network	6		4		6	144
			Signal processing error (corrupted data)	6		4		4	96

Intelligent Electronic Device (IED)	Interface device responsible for collecting data from the electrical equipment and receiving and applying a control command from the operator	failure	Network	6	Communication network becomes unavailable to redirect the important data for the system operation; large volume of data saturating the network capacity; major consumption of processor computation resources. Corrupted communications; Energy systems applications fail or are compromised (non-optimal asset management); decrease in communication network performance	4	Inability to establish communication with IED	5	120
		Monitoring failure	I/O port damage	6	No power component status monitoring. Energy system applications fail or are compromised (non-optimal asset management);	3	Loss of data	3	54
			Significant measurement error	8	Error in monitoring power components. eergy system applications fail or are compromised (non-optimal asset management);	3	Incongruous or corrupted data	2	48
		Control failure	Inability to apply control commands	7	Inability to control power system operation. Energy system applications fail or are compromised;	4	Operational test	1	28
			Inability to apply control commands	7		3	Operational test	1	21
		Power outage	Remote disconnection of power	8	Remote disconnection of power. Energy system applications fail or are compromised; loss of control in the downstream network area;	3	Loss of power	1	24
		Security failure	Hacking for personnel sensitive information	6	Loss of integrity. energy system applications run under fallacious information; loss of integrity;	5	Firewall block; attempt to pass the firewall; existence of corrupted data	8	240
			Faulty information injection (cyberattack)	6		5		8	240

Severity Criteria

Effect	Criteria: Severity of Effect on Product (Customer Effect)	Rank	Effect	Criteria: Severity of Effect on Product (Manufacturing/Assembly Effect)
Failure to Meet Safety and/or Regulatory requirements	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning	10	Failure to Meet Safety and/or Regulatory requirements	May endanger operator (machine or assembly) without warning.
	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning	9		May endanger operator (machine or assembly) with warning.
Loss or Degradation of Primary Function	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation)	8	Major Disruption	100% of product may have to be scrapped. Line shutdown or stop ship
	Degradation of primary function (vehicle operable, but at reduced level of performance)	7	Significant Disruption	A portion of the production run may have to be scrapped. Deviation from primary process including decreased line speed or added manpower
Loss or Degradation of Secondary Function	Loss of secondary function (vehicle operable, but comfort/convenience functions inoperable)	6	Moderate Disruption	100% of production run may have to be reworked off line and accepted
	Degradation of secondary function (vehicle operable, but comfort / convenience functions at reduced level of performance)	5		A portion of the production run may have to be reworked off line and accepted
Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by most customers (> 75%)	4	Moderate Disruption	100% of production run may have to be reworked in station before it is processed
	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by many customers (50%)	3		A portion of the production run may have to be reworked in-station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by discriminating customers (<25%)	2	Minor Disruption	Slight inconvenience to process, operation or operator
No Effect	No discernible effect	1	No effect	No discernible effect

Figure 1 - Severity Criteria [FMAE20]

Occurance Criteria

Likelihood of Failure	Criteria: Occurrence of Cause - DFMEA (Design life/reliability of item/vehicle)	Criteria: Occurrence of Cause - PFMEA (Incidents per items/vehicles)	Rank
Very High	New technology/new design with no history.	≥ 100 per thousand ≥ 1 in 10	10
High	Failure is inevitable with new design, new application, or change in duty cycle/operating conditions.	50 per thousand 1 in 20	9
	Failure is likely with new design, new application, or change in duty cycle/operating conditions.	20 per thousand 1 in 50	8
	Failure is uncertain with new design, new application, or change in duty/operating conditions.	10 per thousand 1 in 100	7
Moderate	Frequent failures associated with similar designs or in design simulation and testing.	2 per thousand 1 in 500	6
	Occasional failures associated with similar designs or in design simulation and testing.	.5 per thousand 1 in 2,000	5
	Isolated failures associated with similar design or in design simulation and testing.	.1 per thousand 1 in 10,000	4
Low	Only isolated failures associated with almost identical design or in design simulation and testing.	.01 per thousand 1 in 100,000	3
	No observed failures associated with almost identical design or in design simulation and testing.	≤ .001 per thousand 1 in 1,000,000	2
Very Low	Failure is eliminated through preventative control.	Failure is eliminated through preventive control.	1

Figure 2 - Occurance Criteria [FMAE20]

Detectability Criteria

Opportunity for Detection	Criteria: Likelihood of Detection by Design Control	Rank	Likelihood of Detection	Opportunity for Detection	Criteria: Likelihood of Detection by Process Control
No detection opportunity	No current design control; Cannot detect or is not analyzed.	10	Almost Impossible	No detection opportunity	No current process control; Cannot detect or is not analyzed

Not likely to detect at any stage	Design analysis/detection controls have a weak detection capability; Virtual Analysis (e.g., CAE, FEA, ect.) is **not correlated** to expected actual operating conditions.	9	Very Remote	Not likely to detect at any stage	Failure Mode and/or Error (Cause) is not easily detected (e.g. random audits)
Post Design Freeze and prior to launch	Product verification/validation after design freeze and prior to launch with **pass/fail** testing (Subsystem or system testing with acceptance criteria such as ride and handling, shipping evaluation, ect.).	8	Remote	Problem Detection Post Processing	Failure Mode detection post-processing by operator through visual/tactile/audible means
	Product verification/validation after design freeze and prior to launch with **test to failure** testing (Subsystem or system testing until failure occurs, testing of system interactions, etc.).	7	Very Low	Problem Detection at Source	Failure Mode detection in-station by operator through visual/tactile/audible means or post-processing through use of attribute gauging (go / no-go, manual torque check, clicker wrench, etc.)
	Product verification/validation after design freeze and prior to launch with **degradation** testing (Subsystem or system testing after durability test, e.g., function check).	6	Low	Problem Detection Post Processing	Failure Mode detection post-processing by operator through use of variable gauging or in-station by operator through use of attribute gauging (go/no-go, manual torque check/clicker wrench, etc.)
Prior to Design Freeze	Product validation (reliability testing, development or validation tests) prior to design freeze using **pass/fail** testing (e.g., acceptance criteria for performance, function checks, etc.).	5	Moderate	Problem Detection at Source	Failure Mode or Error (Cause) detection in-station by operator through use of variable gauging or by automated controls in-station that will detect discrepant part and notify operator (light, buzzer, etc.) Gauging performed on setup and first-piece check (for set-up causes only)
	Product validation (reliability testing, development or validation tests) prior to design freeze using **test to failure** (e.g., until leaks, yields, cracks, etc.)	4	Moderately High	Problem Detection Post Processing	Failure Mode detection post-processing by automated controls that will detect discrepant part and lock part to prevent further processing
	Product validation (reliability testing, development or validation tests) prior to design freeze using **degradation** testing (e.g., data trends, before/after values, etc.).	3	High	Problem Detection at Source	Failure Mode detection in-station by automated controls that will detect discrepant part and automatically lock part in station to prevent further processing.
Virtual Analysis Correlated	Design analysis/detection controls have a strong detection capability. Virtual analysis (e.g., CAE, FEA, etc.) **is highly correlated** with actual or expected operating conditions prior to design freeze	2	Very High	Error Detection and/or Problem Prevention	Error (Cause) detection in-station by automated controls that will detect error and prevent discrepant part from being made.
Detection not applicable; Failure Prevention	Failure cause or failure mode can not occur because it is fully prevented through design solutions (e.g., proven design standard, best practice or common material, etc.)	1	Almost Certain	Detection not applicable; Error Prevention	Error (Cause) prevention as a result of fixture design, machine design or part design. Discrepant parts cannot be made because item has been error proofed by process/product design

Figure 2 - Detectability Criteria [FMAE20]

Bibliograhy

[FMAE20] Retrieved on April 20th from https://quality-one.com/fmea/